# (U) Confidential Human Source Policy Guide

## (U) Federal Bureau of Investigation

## (U) Directorate of Intelligence

## (U) 0836PG

## (U) September 21, 2015

(U) Classified By: C48W25B14

(U) Derived From: Multiple Sources

(U) Declassify On: 20401231

(U) Revised: 05/20/2016

## (U) General Information

(U) Questions or comments pertaining to this policy guide can be directed to:
(U) Federal Bureau of Investigation Headquarters,
Directorate of Intelligence
(U) Division point of contact: Section Chief, HUMINT Operations Section, [redacted]

## (U) Supersession Information

(U) This document supersedes the following:

- (U) [redacted]
- (U) [redacted]
- (U) All electronic communications related to confidential human source operations dated prior to the publication of this policy guide, including:
  - [redacted]

(U) Sections 1-3 of this policy guide contain guidance regarding the use of Type 5 assessments. Sections 4-22 incorporate the current *Confidential Human Source Policy Guide* [redacted], revised September 7, 2007, but with new guidance regarding consensual recording and undisclosed participation to reflect revisions prompted by the *Domestic Investigations and Operations Guide* (DIOG). This policy guide will be updated when guidance regarding confidential human source administration and domestic and international confidential human source operations is finalized.

(U) This document and its contents are the property of the FBI. If the document or its contents are provided to an outside agency, it and its contents are not to be distributed outside of that agency without the written permission of the unit listed in the contact section of this policy implementation guide.

(U) This policy guide is solely for the purpose of internal FBI guidance. It is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable by law by any party in any matter, civil or criminal, nor does it place any limitation on otherwise lawful investigative and litigative prerogatives of the Department of Justice and the FBI.

## (U) DIOG Provision

(U) No policy or policy guide may contradict, alter, or otherwise modify the standards of the DIOG. Requests for DIOG modifications can be made to the Internal Policy office (IPO) pursuant to DIOG subsection 3.2.2 paragraphs (A), (B), (C), and (D).

# (U) Table of Contents

1. (U) Introduction ..... 1
1.1. (U) Scope ..... 1
1.2. (U) Purpose ..... 1
1.3. (U) Intended Audience ..... 1
1.4. (U) Authorities ..... 1
1.5. (U) Approval Levels and Delegations ..... 2
1.5.1. (U) AGG-CHS and AGG-Dom Exceptions and Dispute Resolution ..... 2
1.5.2. (U) CHSPG and DIOG Exceptions and Dispute Resolution ..... 2
2. (U) Roles and Responsibilities ..... 4
2.1. (U) CHS Program Management and Oversight ..... 4
2.1.1. (U) Assistant Directors in Charge, Special Agents in Charge, Assistant Special Agents in Charge (ASACs), and Supervisory Special Agents (SSAs) ..... 4
2.1.2. (U) Confidential Human Source Coordinator (CHSC) ..... 4
2.1.3. (U) Department of Justice Confidential Human Source Coordinator ..... 5
2.2. (U) CHS Operation ..... 5
2.2.1. (U) Case Agent and Co-Case Agent Roles ..... 5
2.2.2. (U) Task Force Officer as Co-Case Agent ..... 6
2.2.3. (U) Non-Agent Investigative Staff ..... 6
2.3. (U) Prohibitions on FBI Personnel in the Identification, Evaluation, and Recruitment of PCHSs and the Development and Operation of CHSs ..... 8
2.3.1. (U) Gifts ..... 10
3. (U) Identification, Evaluation, and Recruitment of Confidential Human Sources in Type 5 Assessments ..... 12
3.1. (U//FOUO) PCHS Risk/Benefit Analysis ..... 12
3.2. (U//FOUO) PCHS Operations: Introduction ..... 13
3.3. (U) Identification Phase ..... 14
3.3.1. (U) Opening the Type 5 Assessment in the Identification Phase ..... 14
3.3.2. (U) Modification of the CHS Identification Plan ..... 15
3.3.3. (U) Transition From the Identification Phase to the Evaluation and Recruitment Phases ..... 16
3.4. (U//FOUO) Evaluation and Recruitment Phases ..... 16
3.4.1. (U//FOUO) Evaluation Phase ..... 16

3.4.2. (U//FOUO) Recruitment Phase ..... 17
3.4.3. (U) Opening the Type 5 Assessment in the Evaluation and Recruitment Phases ..... 17
3.5. (U) Basic Approval: All Phases ..... 18
3.5.1. (U) Additional Approvals ..... 18
3.6. (U) Authorized Investigative Methods in Type 5 Assessments: All Phases ..... 20
3.7. (U) PCHS Approaches ..... 22
3.7.1. (U) Guidance Specific to Special Agents Approaching a PCHS ..... 22
3.7.2. (U) Methods of Approach ..... 22
3.8. (U) File Reviews ..... 31
3.9. (U//FOUO) Funding for Type 5 Assessments ..... 31
3.9.1. (U) Identification Phase Funding ..... 32
3.9.2. (U) Evaluation and Recruitment Phase Funding ..... 32
3.10. (U//FOUO) Duration and Closure of a Type 5 Assessment ..... 33
3.10.1. (U) File Maintenance and Disposition ..... 34
4. (U) Opening and Reopening a Confidential Human Source ..... 35
4.1. (U) Use of the CHS Program ..... 35
4.2. (U) When a CHS May Be Tasked ..... 35
4.3. (U) Source-Opening Communication ..... 35
4.4. (U) Additional Background Information and Records Checks ..... 38
4.5. (U) Requirements for Reopening a CHS ..... 39
4.5.1. (U) Request to Reopen a CHS Previously Closed for Cause ..... 40
4.5.2. (U) Closed CHS Reopened by Another Field Office ..... 40
5. (U//FOUO) Confidential Human Source Admonishments ..... 41
5.1. (U) Timing and Provision of Admonishments ..... 41
5.2. (U) Required Admonishments ..... 41
5.3. (U) Additional Admonishments ..... 41
5.3.1. (U) Subjects Represented by Counsel or Planning Legal Defense ..... 42
5.3.2. (U) Employees of Financial Institutions ..... 42
5.3.3. (U) Employees of Educational Institutions ..... 43
5.3.4. (U) Otherwise Illegal Activity ..... 43
6. (U//FOUO) Confidential Human Sources Requiring Department of Justice Approval for Operation ..... 44
6.1. (U) Types of CHS That Require DOJ Approval ..... 44

6.1.1. (U) Senior Leadership CHSs ..... 44
6.1.2. (U) High-Level Government CHSs ..... 44
6.1.3. (U) High-Level Union Official CHSs ..... 44
6.1.4. (U//FOUO) Privileged CHSs ..... 44
6.1.5. (U) Media CHSs ..... 45
6.1.6. (U//FOUO) Long-Term CHSs ..... 45
6.2. (U) DOJ Review Procedure for CHSs Requiring DOJ Approval ..... 46
6.2.1. (U) CHSs Reporting on National Security and Foreign Intelligence ..... 46
6.2.2. (U) CHSs Not Reporting on National Security Investigations or Foreign Intelligence Collection ..... 47
7. (U//FOUO) Confidential Human Sources Requiring Additional Approvals .... 48
7.1. (U) Federal Probationers, Parolees, and Supervised Releasees ..... 48
7.2. (U) Prisoners Under Bureau of Prisons (BOP) Supervision or in the Custody of the United States Marshals Service (USMS) ..... 48
7.2.1. (U) FPO, BOP, and USMS Approval ..... 48
7.3. (U) State or Local Prisoners, Probationers, Parolees, and Supervised Releasees ..... 49
7.3.1. (U) Approval to Release a State or Local Prisoner From Custody ..... 49
7.4. (U) BOP Personnel ..... 50
7.5. (U) State, Local, or Contract Prison Employees ..... 50
7.6. (U) Sworn Law Enforcement Officers ..... 51
7.7. (U) Employees of Federal, State, Local, or Tribal Agencies ..... 51
7.8. (U) Minors (Individuals Under the Age of 18) ..... 51
7.9. (U) Counselors, Employees, and Patients in Substance Abuse Treatment Programs ..... 51
7.10. (U//FOUO) Union Officials ..... 52
7.11. (U) Department of Energy (DOE) Personnel ..... 52
7.12. (U) Personnel Affiliated With the Department of Defense (DoD) (Not Including Joint Operations With DoD) ..... 52
7.12.1. (U//FOUO) Definitions ..... 53
7.12.2. (U//FOUO) Concurrence Requirements ..... 53
7.12.3. (U//FOUO) Concurrence Procedures ..... 53
7.13. (U) Fugitives ..... 55
7.14. (U) Illegal Aliens ..... 56
7.15. (U) Former FBI Employees and Persons With a Present or Former Relationship With an FBI Employee ..... 56

7.16. (U) Current or Former Participants in the Witness Security Program (WSP) ..... 56
7.17. (U) Members of Congress and Their Staffs ..... 56
7.18. (U) White House Personnel ..... 57
7.19. (U) No Foreign Policy Objection Statement ..... 57
8. (U) Witness Security Program ..... 59
[redacted]
9. (U) Immigration Matters ..... 63
9.1. (U//FOUO) CHSs in the United States Illegally ..... 63
9.2. (U) Requirements for Opening, Operating, and Closing ..... 63
9.3. (U) Available Programs for Acquiring Legal Immigration Status for a CHS and Delaying a CHS's Deportation ..... 63
9.3.1. (U) Significant Public Benefit Parole Program ..... 63
9.3.2. (U) Deferred Action Program ..... 69
9.3.3. (U//FOUO) Advance Parole ..... 70
9.3.4. (U) S Visa Program ..... 71
9.3.5. (U) Public Law 110 (PL-110) Program ..... 73
9.4. (U) Individuals Seeking Asylum ..... 74
9.5. (U//FOUO) Notional Documents ..... 74
10. (U//FOUO) Operation of Confidential Human Sources ..... 75
10.1. (U//FOUO) CHSs Who May Testify in a Court or Other Proceeding ..... 75
10.2. (U) Electronic Communications With a CHS ..... 75
10.3. (U) Consensual Recording ..... 76
10.4. (U) Undercover Operation ..... 76
10.5. (U//FOUO) Undisclosed Participation ..... 76
10.6. (U//FOUO) Alias/False Identification ..... 76
10.7. (U) Obtaining Information About a Subject's Pending Charges or Legal Defense Plans ..... 77

10.8. (U//FOUO) Use of a CHS Associated With a Wire or Electronics Service Provider ..... 77
10.9. (U) Elected or Appointed Government Officials ..... 78
10.10. (U//FOUO) Employees of Financial Institutions ..... 78
10.11. (U//FOUO) Employees of Educational Institutions ..... 78
10.12. (U//FOUO) Use of a Sub-Source ..... 79
10.13. (U//FOUO) Use of CHS Information in a Foreign Intelligence Surveillance Act Affidavit ..... 79
10.14. (U//FOUO) CHS Prioritization System ..... 79
11. (U) Department of Justice Notification Requirements ..... 80
11.1. (U) Notification Designees ..... 80
11.2. (U) Notification to DOJ of Unauthorized Illegal Activity ..... 80
11.3. (U) Notification to DOJ of the Investigation or Prosecution of a CHS ..... 80
11.4. (U) Notification to DOJ Regarding Certain Federal Judicial Proceedings ..... 80
11.5. (U) Notification to DOJ of Privileged or Exculpatory Information ..... 81
11.6. (U//FOUO) Notification to DOJ Upon Naming a CHS as an Interceptee or a Violator in an Electronic Surveillance Application ..... 81
11.7. (U//FOUO) Responding to Requests From FPO Attorneys Regarding a CHS ..... 82
11.8. (U) Exceptions to the DOJ Notification Requirements ..... 82
11.9. (U//FOUO) DOJ Review of CHS Files for Non-Testimonial CHSs ..... 82
12. (U) Confidential Human Source Participation in Unauthorized Illegal Activity ..... 83
12.1. (U) Notification Process ..... 83
12.2. (U//FOUO) Request for Approval of the Continued Operation of a CHS ..... 83
12.3. (U//FOUO) UIA Resulting From Violation of the Authorization for Illegal Activity ..... 84
13. (U//FOUO) Confidential Human Source Participation in Otherwise Illegal Activity ..... 85
13.1. (U) Prohibited Activities ..... 85
13.2. (U) Tier I OIA ..... 85
13.2.1. (U) Tier I OIA Definition ..... 85
13.2.2. (U) Tier I OIA Authorization ..... 86
13.2.3. (U//FOUO) Tier I OIA Emergency Oral Authorization ..... 87
13.2.4. (U) Tier I OIA Duration ..... 87

13.3. (U) Tier II OIA ..... 87
13.3.1. (U) Tier II OIA Authorization ..... 88
13.3.2. (U) Coordination With FPO Attorney ..... 88
13.3.3. (U) Tier II OIA Emergency Oral Authorization ..... 88
13.3.4. (U) Tier II OIA Duration ..... 88
13.4. (U) Documented Findings of Tier I and Tier II OIA Approvers ..... 88
13.4.1. (U) Precautionary Measures ..... 89
13.5. (U) Admonishments Related to OIA ..... 89
13.6. (U) Renewal and Expansion of OIA Authorization ..... 90
13.7. (U) Suspension of OIA Authorization ..... 90
13.8. (U) Revocation of OIA Authorization ..... 90
13.9. (U) Recordkeeping Procedures ..... 91
**14. (U//FOUO) Operation of Confidential Human Sources Involving Other Federal, State, Local, and Tribal Agencies or FBI Field Offices ..... 92**
14.1. (U) Joint Operations of FBI CHSs With Other Agencies ..... 92
14.1.1. (S//NF) Joint Operation With CIA, USG, OR USIC to Advance National Security Objectives ..... 92
14.2. (U) Sole Operation of an FBI CHS by Another Agency ..... 92
14.3. (U//FOUO) Joint Field Office Operation or a CHS Operating Within Another FBI Field Office ..... 93
14.4. (U//FOUO) Operation of CHSs in Another Field Office's Territory ..... 93
**15. (U//FOUO) Disclosure of a Confidential Human Source's Identity ..... 95**
15.1. (U) Principles of Confidentiality ..... 95
15.2. (U) Disclosure Authority ..... 95
15.3. (U//FOUO) SAC Objection to CHS Disclosure Requirement ..... 96
15.4. (U//FOUO) Record of Disclosure of CHS Identity ..... 96
**16. (U//FOUO) Administration of Confidential Human Sources ..... 97**
16.1. (U//FOUO) CHS Files ..... 97
16.1.1. (U//FOUO) Creation and Maintenance of CHS Files in Delta ..... 97
16.1.2. (U//FOUO) Exemption From Creation and Maintenance of CHS Files in Delta ..... 97
16.1.3. (U//FOUO) Opening the CHS on Paper, For Delta Exempt ..... 99
16.1.4. (U//FOUO) Managing the Paper File, For Delta Exempt ..... 99
16.1.5. (U//FOUO) CHS File Structure and Content ..... 99

16.1.6 (U) Properly Classifying CHS Information ..... 100
16.1.7. (U) Documenting CHS Information ..... 100
16.1.8. (U) Retention of CHS Files ..... 101
16.2. (U//FOUO) CHS Number ..... 102
16.3. (U) Payment Name ..... 102
16.4. (U) Code Name ..... 102
16.5. (U//FOUO) CJIS Division/NCIC "Stop Notices" ..... 102
16.6. (U) Positive Records Checks and Concurrence to Operate ..... 102
16.7. (U) Field Office Annual Source Report ..... 102
16.8. (U) Quarterly Supervisory Source Report ..... 103
16.9. (U) Annual Database Checks ..... 103
16.10. (U) Documenting CHS Derogatory Information ..... 103
16.11. (U) Other CHS-Related Deconfliction Checks ..... 103
16.12. (U//FOUO) Transport of CHS Files and Access to Delta Files by Another Field Office or FBIHQ ..... 104
16.13. (U) Requirements When a CHS is Injured or Killed ..... 104
17. (U//FOUO) Confidential Human Source Financial Matters ..... 105
17.1. (U) Payment Prohibitions ..... 105
17.2. (U//FOUO) Field Office Funding for CHSs ..... 105
17.3. (U) SAC Annual CHS Payment Authority ..... 105
17.4. (U) Aggregate Payment Authority ..... 107
17.5. (U) CHS Payment Categories: Services and Expenses ..... 108
17.5.1. (U) Services ..... 108
17.5.2. (U) Expenses ..... 108
17.6. (U) Rules Regarding Expenses for Meals, Vehicles, Medical Costs, Housing, Equipment, and Relocation ..... 109
17.6.1. (U) Meals Associated With CHS Debriefings ..... 109
17.6.2. (U) Vehicles ..... 109
17.6.3. (U) Medical Costs ..... 111
17.6.4. (U) Housing ..... 112
17.6.5. (U) Equipment ..... 112
17.6.6. (U) Relocation ..... 113
17.7. (U) Payment Requests ..... 115

17.7.1. (U) Payment Request Entries ..... 115
17.7.2. (U) Vendor Receipts ..... 116
17.8. (U) Payment Approvals ..... 116
17.8.1. (U) FPO Attorney Approval ..... 116
17.8.2. (U) FBI Field Office Approval ..... 116
17.8.3. (U) Advance Expense Payments ..... 117
17.9. (U) Paying a CHS ..... 117
17.10. (U) SSA Financial Audit of Payments ..... 118
17.11. (U) Acceptable Uses for Service Agreements ..... 119
17.11.1. (U) Modification, Expiration, Renewal, and Termination of Service Agreements ..... 120
17.12. (U) Payments to CHSs by Other Field Offices ..... 120
17.13. (U) Gifts in Lieu of Monetary Payments ..... 121
17.14. (U) Lump-Sum Payments ..... 121
17.15. (U) Rewards ..... 122
17.15.1. (U) Rewards Offered by Entities Outside the FBI ..... 122
17.15.2. (U) Rewards Offered by the FBI ..... 122
17.16. (U) Forfeiture Awards ..... 122
17.17. (U) Project-Generated Income ..... 123
17.18. (U) Funds/Gifts Given to a CHS by a Subject ..... 124
17.19. [redacted] ..... 124
17.19.1. [redacted] ..... 125
17.19.2. [redacted] ..... 127
17.20. (U) Payments to a Closed CHS ..... 127
17.21. (U) One-Time Non-CHS Payment ..... 127
17.22. (U) Payments to a Non-CHS Requiring Maintenance and Security ..... 127
18. (U) Closing a Confidential Human Source ..... 129
18.1. (U) Closing Communication ..... 129
18.1.1. (U) General Reasons for Closing a CHS ..... 129
18.1.2. (U) Closing a CHS for Cause ..... 129
18.2. (U) Closing Procedure ..... 130
18.2.1. (U) Delayed Notification ..... 130
18.3. (U) Future Contact With a Closed CHS ..... 130

18.4. (U) Coordination With FPO Attorneys ..... 130
19. (U) Extraterritorial Operations ..... 132
19.1. (U) National Security Investigations ..... 134
19.1.1. (U) ET CHS Operation in Support of a National Security Investigation ..... 134
19.1.2. (U) Prohibited ET National Security CHS Operations ..... 135
19.2. (U) Required Approvals and Notifications for ET CHS National Security Operations ..... 135
19.2.1. (S//NF) ET OIA by a CHS in Support of a National Security Investigation ..... 137
19.3. (U) Criminal Investigations ..... 140
19.3.1. (U) ET CHS Operations in Support of Criminal Investigations Not Involving Sensitive Circumstances ..... 140
19.3.2. (U) ET CHS Operations in Support of Criminal Investigations Involving Sensitive Circumstances ..... 140
19.3.3. (U) Required Approvals and Notifications for ET CHS Criminal Operations ..... 141
19.3.4. (S//NF) ET OIA by a CHS in Support of a Criminal Investigation ..... 143
19.4. (U) Policy Applicable to ET CHS Operations in Support of All Types of Investigations ..... 145
19.4.1. (U) Documentation Requirements for All CHS ET Operational and Communication Requests ..... 145
19.5. (U//FOUO) Roles of the FBIHQ Operational Entities ..... 155
19.5.1. (U//FOUO) Role of the Operational Division HUMINT Operations Center ..... 155
19.5.2. (U//FOUO) Role of the FBIHQ Operational Unit ..... 157
19.5.3. (U//FOUO) Role of the Directorate of Intelligence HUMINT Coordination Center ..... 157
19.6. (U//FOUO) Role of the Legat in ET CHS Operations ..... 158
19.7. (U//FOUO) Role of the International Operations Division in ET CHS Operations ..... 159
19.7.1. (U) International Operations Division Approval and Management Role Over LEGAT- or ALAT-Assigned ET CHS ..... 160
19.8. (U) ET CHS Operations by a LEGAT or an ALAT ..... 160
19.8.1. (U//FOUO) LEGAT or ALAT Access to a Field Office CHS File ..... 161
19.9. (U) Employee Travel Related to a CHS Operation ..... 161
19.9.1. (S//NF) Special Agent Undeclared Travel ..... 162
19.10. (S//NF) ET Admonishments ..... 163

19.11. (U) Pre-Operational CHS ET Briefs and Planning ..... 164
19.12. (U//FOUO) CHS Payments ..... 164
19.13. (U//FOUO) Emergency ET OIA Authorization ..... 164
19.14. (U) Duration of ET OIA Authorization and Request for Renewal ..... 165
19.14.1. (U) Suspension and Revocation of ET OIA Authorization ..... 165
19.15. (U) Exemption to Providing Legat Notification ..... 165
19.16. (U) Special Circumstances ..... 166
19.17. (U//FOUO) Use of an ET Sub-Source ..... 166
19.18. (U) Communications About a CHS ..... 166
19.19. (U) ET Unauthorized Illegal Activity ..... 166
19.19.1. (U) Unauthorized Illegal Activity Notification to DOJ ..... 167
19.20. (S//NF) International Incidents ..... 168
**20. (U) Confidential Human Source Validation ..... 169**

## (U) List of Appendices

**Appendix A: (U) Final Approvals ..... A-1**
**Appendix B: (U) Sources of Additional Information ..... B-1**
**Appendix C: (U) Contact Information ..... C-1**
**Appendix D: (U) Acronyms ..... D-1**
**Appendix E: (U) TS//SCI CHS Reporting ..... E-1**
**Appendix F: (U) Service Agreement ..... F-1**

# 1. (U) Introduction

## 1.1. (U) Scope

(U//FOUO) The Federal Bureau of Investigation (FBI) recruits and operates confidential human sources (CHSs) to obtain intelligence, which advances investigative program priorities, meets national and FBI intelligence collection requirements, and, through dissemination, supports objectives of the United States (U.S.) government's intelligence and law enforcement (LE) communities. The Directorate of Intelligence (DI) maintains responsibility for these activities through the development and oversight of the FBI's CHS program.

(S//NF) This policy guide (PG) applies to the use of the CHS Program in all investigative and intelligence collection activities conducted by the FBI in the United States, its territories, outside the territories of all countries, and in foreign countries.

(U) The CHSPG is for internal guidance. It is not intended to create an enforceable legal right or a private right of action by a CHS or any other person. Any conflict between these guidelines and the *Attorney General's Guidelines* [AGGs] *Regarding the Use of FBI Confidential Human Sources* [AGG-CHS] or the *Attorney General's Guidelines for Domestic FBI Operations* [AGG-Dom] must be resolved in favor of the AGGs.

## 1.2. (U) Purpose

(U) The purpose of this PG is to standardize CHS Program policies so that they are consistently and uniformly applied, to the extent possible, in all FBI investigative programs. This will promote compliance with relevant AGGs and facilitate the development of CHSs to engage in cross-program reporting.

(U//FOUO) The critical components of the CHS Program addressed in this PG are as follows:

- (U//FOUO) The roles and responsibilities of FBI personnel and task force officers (TFOs) with regard to CHS Program activities
- (U//FOUO) The identification, evaluation, and recruitment of potential confidential human sources (PCHSs)
- (U//FOUO) The administration and operation of CHSs supporting any of the FBI's investigative programs and/or other authorized information collection activities

(U) This PG also emphasizes the importance of oversight and self-regulation to ensure that CHS Program activities are conducted within Constitutional and statutory parameters and that civil liberties and privacy are protected.

## 1.3. (U) Intended Audience

(U) This PG applies to all FBI employees, TFOs, FBI contract employees, and FBI detailees.

## 1.4. (U) Authorities

(U//FOUO) The provisions in this PG are governed by the authorities set forth below.

- (U) *Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources*, December 13, 2006
- (U) *Attorney General's Guidelines for Domestic FBI Operations*, September 29, 2008

- (U) *Domestic Investigations and Operations Guide* (DIOG), October 16, 2011
- (U) Attorney General Order No. 3019-2008, *Conforming the Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources to the Attorney General's Guidelines for Domestic FBI Operations*, November 26, 2008

(U//FOUO) Other authorities, such as statutes, executive orders (EOs), regulations, and memorandums of understanding (MOUs) are referenced in this PG.

### 1.5. (U) Approval Levels and Delegations

(U) Approval levels specified in this PG may be delegated one supervisory level below the stated level or to a designee, unless specifically prohibited in the PG. The delegation must be made in writing, it must specify each activity or task delegated and identify the supervisory position to which the approval authority is delegated. Delegations of authority for senior executives are filed under [redacted] and delegations of authority for non-senior executives are filed under [redacted]. A field office (FO) retaining a communication detailing a delegation of authority must file the delegation of authority communication into the local FO extension of the above [redacted] HQ case file (e.g., [redacted])

(U) All supervisory authority for approval of an activity cited in this PG may be granted by a duly authorized acting supervisor or by a supervisor holding a position higher than that specified in this PG.

(U) References to the special agent in charge (SAC) in this PG are intended to include the FO assistant director in charge (ADIC) position, even if not specifically mentioned.

#### 1.5.1. (U) AGG-CHS and AGG-Dom Exceptions and Dispute Resolution

(U//FOUO) Whenever an FBI assistant director (AD) (or above), ADIC, SAC, chief federal prosecutor (CFP), or his or her respective designee(s) believes that extraordinary circumstances exist that warrant an exception to any provision of the AGG-CHS, or whenever there is a dispute between or among the FBI and other Department of Justice (DOJ) entities regarding the AGG-CHS, an exception must be sought from—or the dispute must be resolved by—the DOJ's assistant attorney general (AAG) (or his or her designee) for the Criminal Division or the National Security Division (NSD), whichever is appropriate.

(U//FOUO) Whenever there is a dispute with the AAG for either the Criminal Division or NSD of the DOJ, the dispute must be resolved by the deputy attorney general (DAG) or his or her designee.

(U//FOUO) Any departure from a provision of the AGG-Dom must be requested and made in accordance with DIOG Section 2.

(U//FOUO) Any exception to a provision of the AGG-CHS must be requested via an electronic communication (EC) with prior approval of the SAC and sent to the AD, DI for review. The AD must coordinate the request for the exception with the appropriate DOJ component.

(U//FOUO) The exception granted or dispute resolved must be documented in the CHS Delta file.

#### 1.5.2. (U) CHSPG and DIOG Exceptions and Dispute Resolution

(U//FOUO) Whenever an ADIC or an SAC believes that extraordinary circumstances exist that warrant an exception, or when there is a dispute over the interpretation of any provision of this

PG, an exception must be sought from, or the dispute resolved by, the AD, DI. The request for exception or dispute resolution must be made via an EC approved by the SAC and AD, DI.

(U//FOUO) Any departure from a relevant provision of the DIOG must be requested and made in accordance with DIOG Section 2.

(U//FOUO) The decision regarding an exemption request or dispute addressed in this subsection must be documented in the CHS's main file.

# 2. (U) Roles and Responsibilities

## 2.1. (U) CHS Program Management and Oversight

### 2.1.1. (U) Assistant Directors in Charge, Special Agents in Charge, Assistant Special Agents in Charge (ASACs), and Supervisory Special Agents (SSAs)

(U//FOUO) The SAC of each FO is responsible for ensuring that the FO has a CHS program that contributes to the FBI's collective human intelligence (HUMINT) base. ADICs, SACs, and members of the FO's investigative and intelligence operations management staff, including ASACs and SSAs, must ensure that the FO fulfills its intelligence collection and information dissemination responsibilities in compliance with FBI protocols, rules, and regulations, including those contained in this PG. Although the SAC is charged with the ultimate responsibility for the FO's CHS program, daily oversight responsibility for PCHSs and CHSs resides with the SSA, who must review all communications regarding the CHSs on his or her squad and supervise the special agents (SAs) operating those CHSs.

(U) SSA program management responsibilities may not be delegated to non-agent personnel. (Supervisory intelligence analysts [SIAs] do, however, have critical oversight responsibilities with regard to the identification and evaluation of PCHSs, as set forth in Section 3, "Identification, Evaluation, and Recruitment of Confidential Human Sources in Type 5 Assessments.")

### 2.1.2. (U) Confidential Human Source Coordinator (CHSC)

(U) Each FO must have at least one SA serving as the FO's full-time CHSC. The CHSC is responsible for addressing all duties and responsibilities of the CHS program. The CHSC must be assigned to the FO's HUMINT squad, [redacted], or intelligence program. At least one alternate CHSC, who need not be assigned to the [redacted] HUMINT, or intelligence squad, must also be designated. The SAC, at his or her discretion, may have additional personnel assigned to these duties, as appropriate.

(U) The CHSC is responsible for overseeing the FO's CHS program, including the proper administration of CHS files and associated documentation. Because of these oversight responsibilities, the CHSC must not be assigned as either the case agent (CA) or co-case agent (co-CA) for any CHS assigned to the FO. This restriction does not apply to the alternate CHSC. However, when the alternate CHSC is working in that capacity, he or she may not review any communication generated for or about CHSs for which the CHSC is the CA or co-CA. These communications must be forwarded for review to the HUMINT and/or [redacted] SSA who supervises the CHSC.

(U//FOUO) Each CHSC must designate a space within the confidential file room (CFR) to house all legacy and current CHS files and other CHS-related material, such as any physical gift received from a CHS that is not considered evidence. In order to guarantee the confidentiality of CHS information, only personnel assigned to the CHS program may be located inside the CFR.

### 2.1.3. (U) Department of Justice Confidential Human Source Coordinator

(U) The AGG-CHS define a CHSC as a supervisory Federal Prosecuting Office (FPO)[1] attorney designated by the CFP to facilitate compliance with the AGG-CHS. Matters routinely handled by the DOJ CHSC include coordinating the FPO's responsibilities under the AGG-CHS, serving as an FBI point of contact (POC) for matters under the AGG-CHS, approving matters under the AGG-CHS on behalf of the FPO when no other FPO attorney is assigned or available, and assisting in handling discovery matters. Each FO CHSC must establish and maintain contact with the DOJ CHSC(s) in his or her territory. Contacts with the DOJ CHSC must be documented and maintained in the CHS program file.

## 2.2. (U) CHS Operation

### 2.2.1. (U) Case Agent and Co-Case Agent Roles

(U//FOUO) The CA of a PCHS or a CHS must be an FBI SA. Each SA, with the exception of the CHSC, has a core responsibility to create and maintain a CHS base to provide vital information supporting FBI investigative and national intelligence priorities. The SAC may grant an exception to this responsibility when an SA is assigned to duties that logically preclude CHS operation. This exception must be documented in a written EC maintained in the FO CHS program management file.

(U//FOUO) In addition to an assigned CA, every CHS must have a co-CA assigned and identified. A co-CA has all the same duties, responsibilities, and file access as the CA. If a TFO is assigned as co-CA, however, there are limitations to his or her duties, as set forth in subsection 2.2.2., "Task Force Officer as Co-Case Agent." The frequency with which the co-CA meets with the CHS is determined by the impact and significance the CHS's reporting has on FBI investigations. If the CHS contributes significantly to an FBI investigation, the co-CA must meet with the CHS more frequently. The frequency that is considered appropriate should be determined by the CA, co-CA, and their SSA; but, in every case, the co-CA must meet with the CHS at least every six months. The meeting must be documented in the CHS file. This requirement may be met through the documentation of a CHS program-related activity through which the co-CA's meeting with the CHS is evident; for example, a source reporting document, an admonishment form, or a payment receipt bearing the co-CA's name.

(U//FOUO) If the CA and co-CA are unavailable, the SSA may designate, on a temporary basis, another co-CA to handle PCHS matters or operate a CHS. Regardless of such temporary designations, however, the CA is responsible for the maintenance and accuracy of PCHS or CHS files assigned to him or her.

(U//FOUO) No member of the FBI's management staff may serve as the CA or co-CA. The only exceptions to this rule are as follows:

- (U//FOUO) Legal attachés (LEGATs) and assistant legal attachés (ALATs) are permitted to operate CHSs as CAs under a modified approval process, as set forth in Section 19.

---

[1] FPOs include any of the following DOJ components: United States Attorney's Office (USAO); the Criminal Division; the NSD; and any other litigation component of DOJ with authority to prosecute federal criminal offenses, including relevant sections of the Antitrust Division, Civil Division, Civil Rights Division, Environmental and Natural Resources Division, and Tax Division.

"Extraterritorial Operations." However, an FBI Senior Executive Service (SES) executive assigned as the LEGAT may not be assigned as the CA or co-CA.

- (U//FOUO) An acting SSA may continue to be assigned as a CA or a co-CA for PCHSs and CHSs for up to 180 days. While the acting SSA is assigned as a CA, communications related to PCHSs and CHSs for which the SSA is the CA must be approved by the ASAC or an SSA whom the ASAC designates. After 180 days have elapsed, the ASAC approving those communications must assign another SA as the CA or co-CA of those PCHSs and CHSs. The reassignment may be made, however, at any time before 180 days have elapsed, as deemed appropriate by the ASAC.

### 2.2.2. (U) Task Force Officer as Co-Case Agent

(U//FOUO) Although they are non-agent personnel, TFOs who have received the requisite clearances to be detailed on an FBI task force may be assigned as co-CAs for PCHSs and CHSs. An SSA may assign a TFO as a co-CA by approving the opening communication, for either a PCHS or a CHS, in which the TFO is named as the co-CA. The SSA's approval also serves as the authority to disclose the PCHS's or CHS's identity to the assigned TFO.

(U//FOUO) Any TFO assigned as a co-CA must be advised of, and follow, all relevant FBI policies regarding the identification, evaluation, and recruitment of PCHSs and the development and operation of opened CHSs, as described in this PG and other relevant policies, including the AGG-Dom, AGG-CHS, and the DIOG.

(U//FOUO) A TFO co-CA has the same duties and access to the PCHS or CHS file as the CA, except as described below. The TFO co-CA may use the PCHS approach methods described in subsection 3.7.2. ("Methods of Approach"), meet with a PCHS, and debrief an open CHS while unaccompanied by a CA, provided that each contact is fully documented by the TFO and placed in the file of the PCHS or CHS for whom the TFO has been approved as co-CA.

(U//FOUO) A TFO co-CA is not permitted to:

- (U//FOUO) Open a Type 5 assessment.
- (U//FOUO) Prepare the source-opening communication or open a CHS in Delta.
- (U//FOUO) Provide admonishments to a CHS. The TFO may be present as a witness when admonishments are reviewed with a CHS; however, the admonishments must be provided by an SA.
- (U//FOUO) Pay a CHS, unless an SA is present as a witness when CHS payments are made. An [redacted] must be submitted by an SA.

### 2.2.3. (U) Non-Agent Investigative Staff

(U//FOUO) Non-agent FBI investigative staff are not permitted to be assigned as CAs or co-CAs for PCHSs and CHSs, unless specifically stated otherwise in this section. A supervisor may assign non-agent investigative staff Sentinel case participant responsibilities that do not require interaction with a PCHS.

#### 2.2.3.1. (U) Non-Agent Linguists

(U//FOUO) Non-agent linguists are not permitted to be assigned as CAs or co-CAs for PCHSs and CHSs. Non-agent FBI linguists are also prohibited from contacting a PCHS or a CHS

without the presence of a CA, a co-CA, or a TFO who has been assigned as a co-CA. A CA or a co-CA may request, in writing (e.g. email, EC), that a non-agent FBI linguist accompany him or her to a CHS debriefing or be present during a PCHS contact. The SSA of the squad with PCHS or CHS oversight and the supervisor of the non-agent FBI linguist respond to the request, by approving or denying it, in writing.

(U//FOUO) The following information must be included in the request:

- (U//FOUO) A description of the requested services
- (U//FOUO) The specific investigation(s) being supported

(U//FOUO) The following factors should be considered prior to approving a request:

- (U//FOUO) The length of time the services will be needed
- (U//FOUO) The purpose of the services
- (U//FOUO) The potential operational or personal security risks resulting from the non-agent linguist interaction with the PCHS or CHS and the steps to mitigate any identified risks

(U//FOUO) This written request and written approval must only be retained in the CHS's main file.

#### 2.2.3.2. (U) Intelligence Analysts (IAs)

(U//FOUO) IAs are not permitted to be assigned as CAs or co-CAs for CHSs. A supervisor may only assign IAs case management or case participant responsibilities that do not require interaction with PCHSs.

(U//FOUO) IAs are prohibited from contacting CHSs without the presence of a CA, a co-CA, or a TFO who has been assigned as a co-CA. A CA or a co-CA may request, in writing (e.g. email, EC), that an IA accompany him or her to CHS debriefings. The SSA of the squad with CHS oversight and the IA's supervisor must respond to the request, by approving or denying it, in writing.

(U//FOUO) The following information must be included in the request:

- (U//FOUO) A description of the requested services
- (U//FOUO) The specific investigation(s) being supported

(U//FOUO) The following factors should be considered prior to approving the request:

- (U//FOUO) The length of time the services will be needed
- (U//FOUO) The purpose of the services
- (U//FOUO) The potential operational or personal security risks resulting from the IA's interaction with the CHS and the steps to mitigate any identified risks

(U//FOUO) This written request and written approval must only be retained in the CHS's main file.

(U//FOUO) An IA may be assigned as a case participant or a case manager to identify and evaluate PCHSs as part of a Type 5 assessment (see Section 3, "Identification, Evaluation, and

Recruitment of Confidential Human Sources in Type 5 assessments," for guidance on Type 5 assessments). However, due to personal safety issues, the fluid nature of operational activities involving interaction with the public, and other policy constraints, IAs are not permitted to engage PCHSs or the public in operational settings during the course of a Type 5 assessment, including in online venues, as described in subsection 3.7.2.5.6., "Use of the Covert Approach by IAs on Publicly Accessible Web Sites."

### 2.3. (U) Prohibitions on FBI Personnel in the Identification, Evaluation, and Recruitment of PCHSs and the Development and Operation of CHSs

(U) For the purposes of this section, FBI personnel includes TFOs acting as co-CAs and any other detailee participating in the operation, oversight, analysis, or recruitment of an FBI CHS or PCHS.

(U) FBI personnel directing, overseeing, or participating in the direction of a CHS or directing, overseeing, or participating in the identification, evaluation, or recruitment of a PCHS are not permitted to:

- (U) Open another FBI employee as a CHS or a PCHS.
- (U) Open an FBI contractor as a CHS, unless the following criteria are met and documented in the main file:
  - (U) In the performance of his or her duties under the contract, the contractor's association as a contractor with the FBI could not reasonably be discerned by someone in the subject's position, unless the subject's knowledge of the relationship is relevant to the assessment or predicated investigation in which the CHS will be used.
  - (U) The use of the contractor as a CHS will not conflict with his or her contractual obligations.
  - (U) The contracting officer's representative (COR) approves the use of the contractor as a CHS.
- (U) Have any role in the operation or oversight of a CHS or a PCHS who is the employee's spouse, significant other, relative, or other person whose relationship to the employee could create the appearance of a personal or professional conflict of interest.
- (U) Engage in sexual or unduly familiar social relationships with any CHS or PCHS.
- (U) Socialize with a CHS or a PCHS, except to the extent necessary and appropriate for operational reasons. Such socialization must be documented in the CHS or PCHS file. Meals with a PCHS for the purposes of evaluation/recruitment or with a CHS during a debriefing are considered appropriate.
- (U) Entertain or meet a CHS or a PCHS at any FBI employee's residence.
- (U) Pay a CHS with personal funds, use a personal credit card for CHS-related expenses, or pay with other personal items of value (e.g., purchase of telephone with personal funds) or with any money not obtained through the [redacted] payment request process, except in exigent circumstances with oral approval of the SSA. If payment is made under exigent circumstances, the oral authorization must be documented in the CHS's payment sub-file.

as soon as practicable, but no more than five business days from the date of oral approval, reimbursement must be sought in accordance with subsection 17.7.1., "Payment Request Entries," or subsection 17.6.5., "Equipment."

- (U) Allow a CHS or a PCHS to distribute contraband (e.g., illegal drugs or stolen property) into the market unless authorized to do so.
- (U) Authorize a CHS to participate in an act of violence, except in self-defense during an emergency to protect his or her own life or the lives of others against wrongful force.
- (U) Authorize a CHS to participate in an act designed to obtain information for the FBI that would be unlawful if conducted by law enforcement officer (LEO) (e.g., breaking and entering, illegal wiretapping, illegal opening or tampering with the mail, or trespass amounting to illegal search).
- (U) Interfere with, influence, or impede any criminal investigation, arrest, prosecution, or civil action in which the CHS or PCHS is a party or a witness. However, an SAC may submit a letter containing facts regarding a CHS's relationship with the FBI to a prosecutor or a court for consideration. Disclosures must be documented in accordance with Section 16, "Administration of Confidential Human Sources."
- (U) Make any promise of immunity to a CHS or a PCHS; make any commitment limiting the use of any evidence by the government; or give the impression that he or she has the authority to do so. However, an SAC may provide a letter to the prosecutor or court stating the facts regarding a CHS's relationship and assistance to the FBI.
- (U) Disclose FBI investigative information to a CHS or a PCHS (e.g., information relating to electronic surveillance [ELSUR], search warrants, indictments and other charging documents, or the identity of other actual or potential subjects or PCHSs or CHSs), other than what is strictly necessary for operational reasons.
- (U) Reveal to a CHS or a PCHS any information relating to any federal, state, or local pending or closed investigation of the CHS or PCHS or his or her friends or relations, including confirming or denying the existence of an investigation, unless authorized to do so by the CFP or his or her designee, after consulting with the SAC. In national security matters, the SAC or his or her designee must consult with the appropriate operational division at FBIHQ and obtain CFP authorization.
- (U) Exchange gifts with a CHS or a PCHS, except as provided for in subsection 2.3.1., "Gifts."
- (U) Provide the CHS or PCHS with anything of more than a nominal value, except pursuant to an approved CHS payment, as authorized by Section 17, "Confidential Human Source Financial Matters," or pursuant to a Type 5 assessment expense, as authorized by Section 3, "Identification, Evaluation, and Recruitment of Confidential Human Sources in Type 5 Assessments."
- (U) Receive anything of more than nominal value from the CHS or PCHS.
- (U) Engage in any business or financial transactions with the CHS or PCHS.

(U) FBI personnel who are directing or overseeing the direction of a PCHS or a CHS must not discuss operational matters related to the FBI's relationship with the PCHS or CHS with anyone else, unless there is a need to share the information.

(U) When interacting with PCHS and CHSs, all FBI employees, including TFO co-CAs and SA CAs, must conduct themselves professionally and in accordance with FBI standards and guidance for FBI employee conduct, including those set forth in the *FBI Ethics and Integrity Program Policy Directive and Policy Guide, 0754DPG*.

### 2.3.1. (U) Gifts

#### 2.3.1.1. (U) Gifts Offered by a CHS or a PCHS

(U//FOUO) If a PCHS or a CHS offers a gift to a CA, a co-CA, or other FBI employee, the CA, co-CA, or other FBI employee should not accept the item. If the PCHS or CHS is aware of the CA or co-CA's FBI affiliation, the CA or co-CA should use the opportunity to diplomatically advise the PCHS or CHS that the relationship is a professional one and that restrictions apply to their interactions. The offer and refusal of a gift must be documented in the PCHS's file or CHS's validation sub-file. Gifts should be refused even from PCHSs recruited through a nonaffiliated approach (see subsection 3.7.2.2., "Nonaffiliated Approach"). This general rule applies because, among other issues, when the CA or co-CA eventually reveals his or her FBI affiliation to the PCHS, the previous acceptance of a gift may become an obstacle to a successful recruitment.

(U//FOUO) In some very limited circumstances, accepting a gift from a PCHS or a CHS may be justified. The CA's SSA must approve the acceptance of such gifts in accordance with the rules set forth in this subsection. If the CA or co-CA takes the gift and the SSA does not approve, the CA or co-CA must return the gift to the PCHS or CHS.

(U//FOUO) If acceptance of the gift is necessary and appropriate for operational reasons, and the refusal of a gift would irreparably damage the relationship and jeopardize the willingness of a PCHS or a CHS to cooperate or continue to cooperate, an SSA may, after concurrence of the chief division counsel (CDC) (considering the legal and ethical issues associated with retaining the gift), authorize the CA or co-CA to accept the gift. The SSA's authorization for the acceptance of the gift, the results of the consultation with the CDC, a description of the gift, and the justification for its acceptance must be documented in the PCHS's file or the CHS's validation sub-file. The SSA must provide authorization in advance if the CA or co-CA is aware that a PCHS or a CHS will offer a gift. Otherwise, the CA or co-CA must obtain authorization and document the gift in Delta as soon as practicable, but no later than five business days from receipt of the gift. This communication also should be used to document the disposition of the gift (discussed below) and the reason why that particular method of disposition was chosen.

(U//FOUO) The SSA must approve one of the methods described below to store or dispose of an accepted gift. Under no circumstances may the gift be kept by an FBI employee. The disposition method will depend on the type of gift and its prospective operational use or treatment as evidence:

- (U//FOUO) If the item is perishable, it must be destroyed. Prior to the destruction of a perishable gift, a photograph must be taken of the item and placed in the main folder of the CHS file, with documentation noting the destruction method and a brief explanation of why the item was destroyed.

- (U//FOUO) If the gift is not perishable and will not be treated as evidence, the CA or co-CA must submit it to the CFR to be maintained as part of the CHS file (e.g., the gift may be placed physically in a serialized 1A envelope/accordion folder, or a "gift" sub-file can be created from the main file) for appropriate storage. If, on a rare occasion, the gift needs to be worn or shown to the PCHS or CHS so as not to jeopardize the relationship during a subsequent contact or debriefing, the gift must be officially charged out of the file. Upon conclusion of the CHS meeting, the gift must be charged back into the CHS file. Upon closing the CHS file, the gift must follow the National Archives and Records Administration (NARA) approved final disposition schedule established for the CHS file.
- (U//FOUO) If the gift is to be treated as evidence, it must follow the same process as any other evidence. See the [redacted]

(U//FOUO) If an FPO is participating in an investigation or a prosecution using the CHS, written notice must be provided to the FPO attorney—in advance, whenever possible—if an SSA approves the acceptance of a gift. A copy of the FPO notification must be retained in the CHS validation sub-file.

#### 2.3.1.2. (U) Gifts Given to CHSs and PCHSs

(U//FOUO) Gifts offered to PCHSs and CHSs may be provided in accordance with subsection 3.9.2., "Evaluation and Recruitment Phase Funding," and subsection 17.13., "Gifts in Lieu of Monetary Payments."

# 3. (U) Identification, Evaluation, and Recruitment of Confidential Human Sources in Type 5 Assessments

## 3.1. (U//FOUO) PCHS Risk/Benefit Analysis

(U//FOUO) The FBI has successfully vetted and recruited CHSs since its inception. A CHS was traditionally, and still is, often identified during the course of an ongoing assessment or predicated investigation, or through routine liaison. As of December 2008, the AGG-Dom, as implemented by the DIOG, provided an additional tool—known as the "Type 5 assessment"—for the identification, evaluation, and recruitment of CHSs. In addition to the DIOG, this section, in conjunction with Section 2, "Roles and Responsibilities," governs the respective roles of SAs and IAs in the identification, evaluation, and recruitment of PCHSs under the Type 5 assessment. The purpose of this section is to give further details regarding the implementation of DIOG subsection 5.6.3.4; however, in the event of a conflict, the DIOG is the controlling authority.

(U//FOUO) Inherent in each Type 5 assessment, or prior to opening any CHS, is the element of determining the potential benefits to be gained through the identification, evaluation, and recruitment of the PCHS, balancing them against the possible operational and other costs associated with the PCHS and ensuring that the benefits outweigh the costs, given the known information and the circumstances involved. If a PCHS is ultimately opened, he or she enters into a relationship with the FBI, and that relationship will forever affect the life of that individual. The PCHS will be either an "FBI source" or a "former FBI source," and in turn, his or her conduct or misconduct will reflect on the FBI. Fairly or unfairly, the FBI will be viewed in the light of that reflection. Therefore, it is important to recognize that decisions and activities undertaken in the identification, evaluation, and recruitment phases are exercises in risk management.

(U//FOUO) Once the PCHS is open, he or she is subject to the guidance provided in Section 20, "Confidential Human Source Validation." Prior to opening each PCHS, agents and analysts must be aware of the need to assess and weigh the risks associated with the PCHS.

(U//FOUO) There is a number of factors to be considered during the identification, evaluation, and recruitment of a PCHS. Documented past activities and observable characteristics can provide insights that point to future control or handling issues, reliability problems, or lack of credibility on the part of the PCHS. Likewise, the PCHS's beliefs, values, and allegiances may reveal motivational platforms that enhance existing benefits and are critical criteria for the agent and analyst to define throughout the Type 5 assessment. These factors, as outlined in the six bullets below, should then be assessed in their totality against the backdrop of each of the five CHS criteria to determine whether the risk in ultimately recruiting the PCHS source is low, medium, or high, and what steps can be taken to mitigate identified risks. A similar evaluation should then be conducted on the potential benefits the CHS is reasonably expected to deliver. The final step is to determine whether the potential benefits outweigh the potential risks and act accordingly.

(U//FOUO) The factors below must be used by analysts and agents to weigh the risks against the benefits involved during the evaluation and recruitment of PCHSs. Each of the factors and, in turn, the CHS criteria, cannot be weighted equally since, for example, a PCHS's access to relevant intelligence or information may outweigh a particular suitability or security risk, especially if such concerns can be adequately mitigated. When evaluating benefits versus risks,

analysts and agents must determine whether the PCHS's placement and access to needed information or intelligence are sufficient to outweigh the risk(s) associated with one or more of the five factors listed below. Factors to be considered include:

- (U//FOUO) The imminent operational need and importance of the desired information.
- (U//FOUO) The likelihood that the PCHS will inform others of the FBI's interest in the PCHS.
- (U//FOUO) The likelihood that any revelation about the FBI's interest in the PCHS will have a minimal adverse affect.
- (U//FOUO) The likelihood that the intelligence or information will be lost.
- (U//FOUO) Whether and how a risk can be mitigated.
- (U//FOUO) Whether the FBI will be able to control the PCHS through existing handling procedures and verify the trustworthiness of the information provided through the existing validation processes.

(U//FOUO) The PCHS criteria are:

- (U//FOUO) **Access**: the individual's placement and sustained ability to acquire information of operational and/or intelligence interest. (In some instances, this may be a matter of potential access to high-value information.)
- (U//FOUO) **Suitability**: the individual's character, intelligence, and competence as they relate to his or her potential to provide authentic, accurate, and reliable information. This helps to answer the question, "Does the individual have the appropriate attributes to perform as a CHS?"
- (U//FOUO) **Susceptibility**: the likelihood that the individual will accept recruitment as an FBI source and provide information on a confidential manner. This aspect requires an analysis of possible motivations and biases, life experience, and other factors relevant to the willingness of the individual to become a CHS.
- (U//FOUO) **Accessibility**: the FBI's ability to gain access to the individual for the purpose of assessment and evaluation as a means to move toward recruitment.
- (U//FOUO) **Security**: the FBI's assessment of operational security and counterintelligence risks associated with the PCHS. This means evaluating the individual and the operational circumstances related to the following questions:
  - (U//FOUO) What if the individual rejects recruitment by the FBI?
  - (U//FOUO) What if the individual becomes aware of the FBI interest and objectives, but his or her loyalties are elsewhere?
  - (U//FOUO) Are there possible lifestyle or professional vulnerabilities that might create reliability issues or invite exploitation by others?

### 3.2. (U//FOUO) PCHS Operations: Introduction

(U//FOUO) The Type 5 assessment consists of three phases. The identification phase is opened without a specific, named individual, for the purpose of identifying persons with placement and

access from a pool of unknown individuals. The evaluation phase is opened on a specific, named individual believed to have appropriate placement and access, for the purpose of obtaining information to better ascertain the nature and extent of his or her access, security risk, suitability, accessibility, and/or susceptibility to becoming a CHS. The recruitment phase, which is a continuation of the evaluation phase for SAs, involves the SA's efforts to obtain a specific, named individual's agreement to voluntarily enter a relationship with the FBI in order to provide operational assistance and/or intelligence. These phases are addressed in detail in the subsections that follow.

(U//FOUO) The [redacted] and the FO collection management coordinator (CollMC) must be assigned as case participants in every Type 5 assessment.

(U//FOUO) A Type 5 assessment, in any phase, may not be opened on a subject of a pending FBI predicated investigation. In addition, a previously opened CHS may not be opened as a Type 5 assessment. See DIOG Classified Appendix G for a specific exception to this requirement.

### 3.3. (U) Identification Phase

(U//FOUO) The purpose of the identification phase of the Type 5 assessment is to identify a PCHS with placement and access from a pool of unknown individuals.

#### 3.3.1. (U) Opening the Type 5 Assessment in the Identification Phase

(U//FOUO) The approval requirements to open a Type 5 assessment in the identification phase are specified in subsection 3.5., "Basic Approval: All Phases." The Type 5 assessment identification phase is initiated with the submission of a CHS identification plan, which must support an existing predicated investigation or assessment. The plan must be documented in an EC (or a successor form in Delta) using the appropriate [redacted]. The identification phase may be undertaken by an SA assigned to either a HUMINT or an investigative squad, or by an IA assigned to an FO or to FBIHQ who wishes to open a Type 5 assessment in the identification phase. These files may be assigned jointly to SAs and IAs. The 819 classification consists of the following restricted alphas, which specify the operational program area to be supported by the CHS identification plan:

| DT (Domestic Terrorism) | CI (Counter-intelligence) | CYB (Cyber) | CRIM (Criminal) | IT (International Terrorism) | WMD (Weapons of Mass Destruction) | PFI (Positive Foreign Intelligence) |
|---|---|---|---|---|---|---|
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |

(U//FOUO) The contents of the identification plan EC must include the following:

- (U//FOUO) **Case ID:** the designator for the appropriate [redacted] classification
- (U//FOUO) **Title:** CHS Identification Plan
- (U//FOUO) **Synopsis:** the authorized purpose and clearly defined objective(s) of the CHS identification plan
- (U//FOUO) **Details:**

- (U//FOUO) The particular placement and access to information that the FBI is seeking and why the FBI is seeking a person with such placement and access. The identification plan must include the file number(s) and title(s) of the assessment(s) or predicated investigation(s) the Type 5 assessment supports.
- (U//FOUO) Common characteristics or search criteria of individuals believed to have the desired placement and access described above and the basis for selecting the particular characteristics or search criteria. There must be an articulated reason to believe that the characteristics and search criteria will yield the individuals likely to have the desired placement and access, and the selected characteristics must not be based solely on race, ethnicity, national origin, religion, activities protected under the First Amendment, or a combination of only these factors.
- (U//FOUO) The investigative methods the IA or SA anticipates using (e.g., database and online searches, surveillance of physical locations, or attendance at particular events, only as authorized in the DIOG) and the reasons why these investigative methods are expected to yield persons who are likely to have the needed placement and access associated with the common characteristics or search criteria set forth above.

(U//FOUO) In developing the identification plan, the focus should be to understand the activities associated with the threat based upon existing intelligence or information received, and the type or characteristics of people who logically intersect with those activities. From this group, characteristics or search criteria can be refined, and investigative methods identified, to yield specific persons with the appropriate placement and access.

### 3.3.2. (U) Modification of the CHS Identification Plan

(U//FOUO) If an IA or an SA seeks to utilize additional characteristics or investigative methods that were not documented in the identification plan EC, their use must be requested in an EC (or a successor form in Delta) addressing the following:

- (U//FOUO) **Case ID:** the designator for the appropriate [redacted] classification
- (U//FOUO) **Title:** Modification of CHS Identification Plan
- (U//FOUO) **Synopsis:** "To request modification of CHS identification plan created to... [restate the authorized purpose and clearly defined objective(s) of the original CHS identification plan]"
- (U//FOUO) **Details:** the additional characteristics, the reason for selecting them, and the additional investigative methods to be used, with an explanation of how these methods are expected to yield persons with the characteristics specified

(U//FOUO) For more information regarding the definition of the individuals and groups that qualify as sensitive PCHSs, it is important to also refer to Section 5 of the DIOG on Type 5 assessments and Section 10 of the DIOG on sensitive investigative matters (SIMs) in Type 5 assessments.

### 3.3.3. (U) Transition From the Identification Phase to the Evaluation and Recruitment Phases

(U//FOUO) If a CHS identification plan leads to the identification of one or more individuals who appear to have the desired access and placement to be considered for further evaluation and/or recruitment, one of the following steps must be taken:

- (U//FOUO) If the Type 5 assessment in the identification phase was assigned to an IA, the IA must open a separate Type 5 assessment in the evaluation phase (in accordance with subsection 3.4., below) to evaluate the individual as a PCHS.
- (U//FOUO) If the Type 5 assessment in the identification phase was assigned to an SA, one of the following processes must be used:
  - (U//FOUO) The SA may close the Type 5 assessment, and then open and operate the individual as a CHS in accordance with Section 4, "Opening and Reopening a Confidential Human Source," provided that the SA believes that the individual is suitable, the individual agrees to be a CHS, and admonishments are provided to the CHS within 90 days of opening.
  - (U//FOUO) The SA may open a Type 5 assessment in the evaluation or recruitment phase (in accordance with subsection 3.4., below) if additional evaluation or recruitment efforts beyond 90 days are required.

## 3.4. (U//FOUO) Evaluation and Recruitment Phases

(U//FOUO) The approval requirements to open a Type 5 assessment in the evaluation and recruitment phases, which focus on identified individuals, are specified in subsection 3.5., "Basic Approval: All Phases." These individuals may come to the attention of IAs and SAs in a number of ways, including the identification phase of a Type 5 assessment, authorized investigative methods used by SAs in other assessments and predicated investigations, and research of historical information in existing records, as set forth in subsection 3.6., "Authorized Investigative Methods in Type 5 Assessments: All Phases."

### 3.4.1. (U//FOUO) Evaluation Phase

(U//FOUO) The purpose of the evaluation phase of the Type 5 assessment is to obtain additional background information regarding a known individual to better ascertain his or her placement, access, security risk, suitability, and/or susceptibility to becoming a CHS. This phase may be used by IAs and SAs assigned to HUMINT or investigative squads, and by IAs assigned to FBIHQ. SAs may be assigned jointly with IAs to Type 5 assessments in this phase.

(U//FOUO) A Type 5 in the evaluation phase is not a prerequisite to opening an individual as a CHS; rather, the Type 5 provides additional tools that may be used to evaluate a PCHS. An SA may open an individual as a CHS if the SA has sufficient knowledge to believe that the individual has access to valuable information, is susceptible to becoming a CHS, and may be given admonishments within 90 days of opening. However, if an SA focuses on an individual as a PCHS, and the SA requires more than 90 days to evaluate the individual or needs to use investigative methods to further evaluate the individual, an evaluation phase must be opened.

(U//FOUO) IAs and SAs must open an evaluation-phase Type 5 assessment to assess a PCHS, whether the individual was identified through an identification-phase Type 5 assessment or through other means. If an IA develops information during this phase indicating that the PCHS

should be recruited, the IA should prepare a source identification package (SIP) for use in the recruitment of this individual by an SA on the appropriate HUMINT or investigative squad. A SIP is defined as a written product drafted for the purpose of providing information regarding an individual that will be used in order to determine or relay the individual's potential as a CHS. Drafting a SIP is recommended, but not mandatory, because a SIP may not be necessary in all circumstances. However, as stated above, an evaluation-phase Type 5 assessment must be opened before a SIP may be drafted, even if the information used for drafting the SIP was obtained pursuant to an already-open predicated case on the individual, before the focus on him or her was as a PCHS. A CHS targeting package is a SIP; however, the title SIP must be used instead of the targeting package in order to provide consistency across the FBI. Once the SIP is completed, the Type 5 assessment (in the recruitment phase) must be reassigned to the appropriate HUMINT or investigative squad for recruitment.

(U//FOUO) If the information developed during this phase indicates that the individual should not be recruited as a CHS, the Type 5 assessment must be closed in accordance with the DIOG and subsection 3.10., "Duration and Closure of a Type 5 Assessment."

(U//FOUO) SAs may open evaluation-phase Type 5 assessments on individuals identified through identification-phase Type 5 assessments, predicated investigations, or other means, but have the additional authority to engage in recruitment activities under the recruitment phase, which is described below.

### 3.4.2. (U//FOUO) Recruitment Phase

(U//FOUO) The purpose of the recruitment phase of the Type 5 assessment is to obtain a PCHS's agreement to voluntarily enter a relationship with the FBI and provide operational assistance and/or intelligence. Only SAs assigned to investigative or HUMINT squads may engage in the recruitment phase. Non-agent professional staff may be requested to assist with the recruitment phase in accordance with subsection 2.2.3., "Non-Agent Investigative Staff." If the recruitment is successful, the Type 5 assessment must be closed in accordance with the DIOG, and the individual must be opened as a CHS in Delta. The Type 5 assessment must also be closed if the recruitment is not successful, either because the individual declines to become a CHS or a decision is made not to continue the recruitment.

### 3.4.3. (U) Opening the Type 5 Assessment in the Evaluation and Recruitment Phases

(U//FOUO) A Type 5 assessment in the evaluation or recruitment phase must be opened with an EC (or a successor form in Delta) containing the appropriate [redacted] file number. The [redacted] is a set of restricted files consisting of numerical classifications corresponding to specific program areas which the PCHS, based upon placement and access to information on a potential or existing threat, is expected to support if opened as a CHS. These file classifications are set forth in the following table:

| DT | CD | CYB | CID | IT | WMD | PFI |
|---|---|---|---|---|---|---|
| [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] | [redacted] |

(U//FOUO) The contents of the opening EC must include the following:

- (U//FOUO) **Case ID**: the designator for the appropriate [redacted] file

- (U//FOUO) **Title**: the name of the PCHS
- (U//FOUO) **Synopsis**: the authorized purpose and clearly defined objective(s)
- (U//FOUO) **Details**:
  - (U//FOUO) File classification(s) or crime problem indicator (CPI) code(s) of the operational program or threat the PCHS is expected to support
  - (U//FOUO) The PCHS's name, date of birth, and all other available biographical data
  - (U//FOUO) Synopsis of any information collected regarding the PCHS pursuant to an identification-phase Type 5 assessment or a prior assessment or predicated investigation in which the PCHS was initially identified as a subject
  - (U//FOUO) The information for which the PCHS has placement and access, and why such a CHS would be of value to the FBI

### 3.5. (U) Basic Approval: All Phases

(U//FOUO) A Type 5 assessment for any phase must be approved by the appropriate supervisor and opened with an EC (or a successor form in Delta). Notwithstanding any other provision in the DIOG, a Type 5 assessment cannot be opened based on oral approval. An SA opening a Type 5 assessment must obtain SSA approval; an IA opening a Type 5 assessment must obtain approval from the SIA and the SSA on the HUMINT or investigative squad which would eventually recruit any individual identified as a PCHS.

#### 3.5.1. (U) Additional Approvals

(U//FOUO) In addition to the approvals set forth in subsection 3.5. above, additional approvals are required if, during the identification phase, at least one of the characteristics in the subsections below is being used to identify individuals with placement access or is a characteristic of a PCHS in a Type 5 assessment evaluation or recruitment phase. The characteristics are presented according to the approval levels required.

##### 3.5.1.1. (U) CDC Review and SAC Approval for Sensitive PCHSs

(U//FOUO Sensitive PCHSs must be treated in accordance with DIOG subsection 5.6.3.4.4.2.

(U//FOUO) CDC review and SAC approval are required before a Type 5 assessment may be opened on a sensitive PCHS or if, during the identification phase, a sensitive characteristic is at least one of the aspects being used to identify individuals with potential placement and access to information of interest. If it is determined, after opening a Type 5 assessment, that a PCHS is sensitive or that a sensitive characteristic must or will be added to the PCHS identification plan, the assessment activity may continue, but the matter must be documented in an EC (or a successor form in Delta) and reviewed by the CDC and approved by the SAC promptly (i.e., not more than five business days after the determination is made).

(U//FOUO) Sensitive PCHSs (and sensitive characteristics included as part of a CHS identification plan) include:

- (U//FOUO) Domestic public officials (other than members of the U.S. Congress and White House staff, who require higher approval authority—see subsections 3.5.1.2.1. and 3.5.1.2.2., below).

- (U//FOUO) Domestic political candidates
- (U//FOUO) Individuals who are prominent within religious organizations
- (U//FOUO) Individuals who are prominent within domestic political organizations
- (U//FOUO) Members of the news media
- (U//FOUO) Members of faculty or administration of colleges and universities in the United States

### 3.5.1.2. (U) SAC and Executive Assistant Director (EAD) Approval After Consultation With the Office of the General Counsel (OGC)

#### 3.5.1.2.1. (U) White House Personnel

(U//FOUO) SAC and appropriate EAD approval, with a recommendation from the OGC, are required to open a Type 5 assessment in which:

- (U//FOUO) White House staff status is one of the specified characteristics in the CHS identification plan (identification phase).
- (U//FOUO) A member of the White House staff will be evaluated or recruited as a PCHS (evaluation and recruitment phases).

#### 3.5.1.2.2. (U) Members of Congress and Their Staff

(U//FOUO) SAC and appropriate EAD approval, with a recommendation from the OGC and prior notice to the AD, Office of Congressional Affairs (OCA), are required to open a Type 5 assessment in which:

- (U//FOUO) Status as a member of Congress or a part of a member's staff is a specified characteristic in a CHS identification plan (identification phase).
- (U//FOUO) A member of Congress or a part of a member's staff will be evaluated or recruited as a PCHS (evaluation and recruitment phases).

### 3.5.1.3. (U) SAC and Responsible DI Deputy Assistant Director (DAD) Review and Approval

(U//FOUO) SAC approval, [redacted] review, and the approval of the DI DAD with HUMINT program responsibility are required for CHS identification plans and evaluation- and recruitment-phase activity that involve:

- (U//FOUO) The establishment of an apparent or actual business.
- (U//FOUO) The use of employment sites.
- (U//FOUO) Any other activity which might have an adverse legal impact on a third party.

(U//FOUO) Following SAC approval, the request to approve a CHS identification plan for one of the above characteristics must be sent to the [redacted] with a copy to the appropriate [redacted] unit to be presented to the DI review committee.

### 3.5.1.4. (U) Department of State (DOS) Approval

(S//NF) Pursuant to the [redacted]

[redacted]

[redacted]

(S//NF) If the SA conducting the Type 5 assessment determines that an interview is likely to culminate in a recruitment offer, [redacted] must be obtained prior to conducting the interview.

(S//NF) To obtain [redacted] the CA must provide the appropriate FBIHQ operational unit with an SSA-approved EC containing the following information:

- (S//NF) The PCHS's nationality and citizenship
- (S//NF) The time frame of the approach
- (S//NF) The individual's diplomatic or official status
- (S//NF) A description of the individual, including the location and name of the international organizational component or diplomatic establishment to which the PCHS belongs and a description of his or her duties within the organization
- (S//NF) Whether the approach would be passive or coercive
- (S//NF) The target against whom the PCHS is expected to report
- (S//NF) The probable motivation for the PCHS to become a CHS
- (S//NF) If known, whether the PCHS is likely to cooperate

(U//FOUO) The operational unit must then request [redacted] from the DOS before the CA conducts the initial interview.

### 3.6. (U) Authorized Investigative Methods in Type 5 Assessments: All Phases

(U) As set forth in the DIOG, only the investigative methods listed below may be used in a Type 5 assessment, whether in the identification, evaluation, or recruitment phase.

(U) All of the following investigative methods may be used by SAs. IAs may use only the first six investigative methods.

- (U//FOUO) Use of public information
- (U//FOUO) Use of FBI and DOJ records or information

- (U//FOUO) Use of records or information from other federal agencies and state, local, tribal, or foreign government agencies
- (U//FOUO) Use of online services and resources
- (U//FOUO) Use of information voluntarily provided by governmental or private entities
- (U//FOUO) Use of alias/false identification (AFID) or the covert approach (see subsection 3.7.2.5.6., "Use of the Covert Approach by IAs on Publicly Accessible Web Sites," for IA-specific guidance) only permitted for use during approved activity in a Type 5 assessment
- (U//FOUO) CHS use and recruitment
- (U//FOUO) Interviews of or requests for information from the public and private entities
- (U//FOUO) Physical surveillance (not requiring a court order)
- (U//FOUO) Polygraph examinations
- (U//FOUO) Trash covers (i.e., searches that do not require a warrant or court order; SSA approval and consultation with CDC/OGC is required prior to using this method [see DIOG subsection 18.6.12.5])

(U//FOUO) DOJ has opined that SAs are authorized to perform consent searches in assessments.

(U//FOUO) Investigative methods used during assessments that may require higher than SSA approval are set forth in DIOG subsection 18.5.

(U//FOUO) In addition, as specified in division PGs, there may be agreements (e.g., MOUs) that require additional coordination and approval prior to conducting certain activities.

(U//FOUO) In the course of a predicated investigation, an agent may not utilize undercover activity (pursuant to *The Attorney General's Guidelines on Federal Bureau of Investigation Undercover Operations* [AGG-UCO]) with the specific purposes of identifying, evaluating, or recruiting a PCHS. The agent must open a Type 5 assessment and, if deemed operationally appropriate and necessary based upon the circumstances, may seek approval to utilize the covert approach. The following example illustrates this requirement:

> (U//FOUO) **Scenario:** During a predicated investigation of a violent crime group, the FBI CA identifies a person associated with the criminal group who may be a PCHS. Based upon this, the CA decides, according to the AGG-UCO, to use up to "five undercover activity" contacts with the PCHS as a means to evaluate the person as a PCHS.
>
> (U//FOUO) **Response:** This is not permitted. A Type 5 assessment must be opened, and approval to utilize the covert approach can be sought (see CHSPG for approval standards) to further evaluate and recruit the PCHS. The predicated case cannot be used as a basis for undercover activity related to contact with the person, since the actual purpose for the interaction is to evaluate and potentially recruit the person as a CHS rather than seeking information relevant to a federal crime or national security threat.

## 3.7. (U) PCHS Approaches

### 3.7.1. (U) Guidance Specific to Special Agents Approaching a PCHS

(U//FOUO) During the course of a Type 5 assessment, in addition to access to publically accessible Web sites, an SA is allowed to make direct contact with a PCHS as part of the evaluation and recruitment process. All contacts must be documented in an [redacted] "Form for Reporting Information That May Become the Subject of Testimony," which must be retained in the [redacted] file (or a successor file in Delta). In place of the true name of the PCHS, the individual should be referenced in the [redacted] as "PCHS." The [redacted] number should appear on the [redacted] and, if the PCHS provides incidentally collected intelligence, the file number of the relevant assessment or predicated investigation that the information or intelligence supports should be included as well.

(U//FOUO) The sole purpose of an SA's contact with a PCHS during a Type 5 assessment must be to ascertain the PCHS's placement, access, suitability, susceptibility to becoming a CHS, and any security issues that may impact the PCHS. Contact with a PCHS must not be used to task the PCHS to collect evidence or operational intelligence. Only an open CHS who has received the admonishments required in Section 5, "Confidential Human Source Admonishments," may be tasked with collecting evidence or intelligence.

(U//FOUO) In addition, in the course of a predicated investigation, an agent may not utilize undercover activity (up to five substantive contacts pursuant to AGG-UCO), with the specific purpose of identifying, evaluating, or recruiting a PCHS. The agent must instead open a Type 5 assessment and, if deemed operationally appropriate and necessary based upon the circumstances, may seek approval to utilize the covert approach. See subsection 3.7.2.3, "Covert Approach Using True Name," and subsection 3.7.2.5, "Covert Approach," for covert approach guidelines.

> (U//FOUO) **Scenario:** During a predicated investigation of a violent crime group, the FBI CA identifies a person associated with the criminal group who may be a PCHS. Based upon this, the CA decides, in accordance with the AGG-UCO, to use up to "five undercover activity" contacts with the PCHS as a means to evaluate the person as a PCHS.
>
> (U//FOUO) **Response:** This is not permitted. A Type 5 assessment must be opened and approval to utilize the covert approach can be sought to further evaluate and recruit the PCHS. The predicated case cannot be used as a basis for "undercover activity" related contact with the person, since the actual purpose for the interaction is to evaluate and potentially recruit the person as a CHS rather than to seek information relevant to a federal crime or national security threat.

### 3.7.2. (U) Methods of Approach

(U//FOUO) The three types of approaches discussed below are available to an SA during a Type 5 assessment. The approach selected will depend on the SA's planned recruitment strategy. For any of the approaches utilized, if the SA has been issued an AFID, the SA may use the AFID to pay for appropriate recruitment expenses (e.g., meals or event tickets) so as not to disclose his or her FBI affiliation to the vendors or merchants, in accordance with DIOG subsection 18.5.6.4.9. Authorization for incurring expenses in support of recruitment is addressed in subsection 3.9.2, "Evaluation and Recruitment Phase Funding."

(U//FOUO) An SA contacting the PCHS using the nonaffiliated or covert approach must continuously evaluate the need for continued contacts with the PCHS to ensure that those contacts further inform the objectives of the Type 5 assessment (i.e., that additional nonaffiliated or covert contacts provide useful and necessary insight into the PCHS's access, suitability, susceptibility, accessibility, and possible operational security issues).

(U//FOUO) During a Type 5 assessment, the SA may collect information that is volunteered or provided incidentally by the PCHS if it relates to an ongoing assessment, predicated investigation, collection requirement, or other aspect of the FBI's mission. The SA must document this information in an [redacted] filed in the appropriate investigative file, as well as in the [redacted] file (or a successor file in Delta). The SA may also ask questions related to information of interest to the Type 5 assessment (i.e., information for the purpose of ascertaining the PCHS's placement, access, suitability, susceptibility, and accessibility or security concerns).

### 3.7.2.1. (U//FOUO) Affiliated Approach

(U//FOUO) In the affiliated approach, the SA or TFO discloses his or her affiliation with the FBI to the PCHS. The SA or TFO has the option of not revealing the true purpose of the contact to the PCHS. In this affiliated approach option, the PCHS is provided a plausible reason for the contact other than the FBI's purpose of assessing the person as a PCHS. If the true purpose of the contact is not revealed, the SA or TFO must ensure that the purported purpose used would not reasonably be expected to violate the rights or damage the reputation of another person, and that the purported purpose does not imply that adverse legal consequences may follow to the PCHS (or a person close to the PCHS) if the PCHS declines to speak with the SA or TFO.

#### 3.7.2.1.1. (U//FOUO) Approval for Affiliated Approach

(U//FOUO) No approval is required for using the affiliated approach.

### 3.7.2.2. (U//FOUO) Nonaffiliated Approach

(U//FOUO) In the nonaffiliated approach, the SA does not volunteer to the PCHS that he or she is employed by the FBI or other LE or intelligence agency, and a TFO does not volunteer that he or she is employed by the parent LE or intelligence agency or the particular FBI investigative entity, such as a Joint Terrorism Task Force (JTTF). However, the SA or TFO does not use an alias and does not affirmatively deny affiliation with the FBI or other LE or intelligence agency when using this approach. Affirmative denial constitutes the use of the covert approach and includes the use of apparel or props (e.g., wearing a plumber's uniform or driving a cable truck) to intentionally misdirect the SA's or TFO's affiliation with the FBI or other LE or intelligence agency. An SA or a TFO may withhold FBI affiliation if, based upon the operational circumstances, the withholding is necessary or advantageous to achieving the objectives of the assessment. The SA may continue to make contact with the PCHS while using the nonaffiliated approach, as long as the standards set forth below for maintaining nonaffiliation in the Type 5 assessment are met.

(U//FOUO) If the PCHS asks whether the SA or TFO is employed by the FBI or another LE or intelligence agency, and the SA or TFO affirmatively denies the affiliation, the SA may complete the contact with no additional authority. If the SA intends, while using true name, to continue to make these representations in the next substantive contact (meaning, a contact that is not made for the purpose of or related to scheduling the next meeting), the SA must first meet the requirements set forth in subsection 3.7.2.3., "Covert Approach Using True Name." If, however,

the SA intends to affiliate during the next substantive contact, the covert approach requirements do not have to be met.

(U//FOUO) Inherent in utilizing the nonaffiliated approach is not revealing the true purpose of the contact with the PCHS (i.e., that of assessing the person as a PCHS). Therefore, according to the standards for the use of the nonaffiliated approach, the SA must ensure that the purported purpose for contacting the PCHS:

- (U//FOUO) Is plausible.
- (U//FOUO) Would not reasonably be expected to violate the rights or damage the reputation of another person.
- (U//FOUO) Does not imply that adverse legal consequences may follow if the PCHS declines to speak with the SA.

(U//FOUO) Moreover, withholding FBI affiliation (i.e., nonaffiliation) is permitted only if doing so would not reasonably be expected to violate the rights or damage the reputation of another person or entity or have a reasonably anticipated adverse legal consequence.

#### 3.7.2.2.1. (U//FOUO) Approval for Nonaffiliated Approach

(U//FOUO) No supervisory approval is required for utilizing the nonaffiliated approach. However, since achieving the assessment objectives may take time and involve multiple interactions with the PCHS, the CA must continually evaluate the need to withhold affiliation.

### 3.7.2.3. (U//FOUO) Covert Approach Using True Name

(U//FOUO) The covert approach using true name provides a transition mechanism for a SA or a TFO to continue contact with a PCHS, during the evaluation and/or recruitment phases, based upon an articulated basis for doing so while maintaining a nonaffiliated status, and as long as withholding the affiliation would not reasonably be expected to violate the rights or damage the reputation of another person or entity or have a reasonably anticipated adverse legal consequence.

(U//FOUO) There may also be circumstances when an SA plans in advance to use this approach prior to contacting the PCHS.

(U//FOUO) In either of the above circumstances, the requirements for using the covert approach with true name must be met (see subsection 3.7.2.3.1., below).

(U//FOUO) In order to protect the technique, if used, it is generally anticipated that, when using the covert approach with his or her true name, the SA will not later affiliate by disclosing his or her employment with the FBI, but rather will hand off the PCHS to another SA for further evaluation and an affiliated recruitment. However, with appropriate justification and approval, an SA using the covert approach with true name may affiliate by revealing his or her true employment if doing so will not harm or undermine the relationship built with the PCHS, and if it is consistent with assessment objectives (see subsection 3.7.2.3.4., "Transitioning From the Covert Approach Using True Name to the Affiliated Approach").

#### 3.7.2.3.1. (U//FOUO) Covert Approach Using True Name Requirements

(U//FOUO) Generally, the covert approach using true name is utilized in a situation where, during contact with a PCHS, the CA employs the nonaffiliated approach, but finds it necessary during that contact to represent, either affirmatively or through denial, that his or her

employment is something other than as a LEO or a person in a comparable position in the IC. In this first situation, if the CA intends to continue to make these representations in the next substantive contact, the CA must obtain prior approval for subsequent contacts through a written request, as set forth in subsection 3.7.2.3.2, below. In addition, the SA must have successfully completed the [redacted] or an equivalent, [redacted] approved training course. Otherwise, the SA has the option of affiliating during the next meeting with the individual or PCHS or handing off the PCHS to another CA for further evaluation.

(U//FOUO) The second situation in which this technique is appropriate is when the CA plans in advance to use this approach, prior to the first contact with the individual or PCHS. In this situation, the SA must request and obtain prior written approval according to the procedures set forth in subsection 3.7.2.3.2, below. In addition, the SA must have successfully completed the [redacted] or an equivalent, [redacted] approved training course.

#### 3.7.2.3.2. (U//FOUO) Request to Use the Covert Approach Using True Name

(U//FOUO) A request to use the covert approach using true name must be submitted for approval via EC (or successor form in Delta), as detailed below. If the SA anticipates the need for the approach before the Type 5 assessment is opened, the request for the approach should be included in the Type 5 opening document. If the need for this approach arises later, the request must be made in a separate EC (or successor form in Delta). For example, this circumstance might occur if the SA utilizes a nonaffiliated approach in a pending Type 5 assessment but, during the contact, finds it necessary to represent, either affirmatively or through denial, that his or her employment is something other than as a LEO or a person in a comparable position with the United States Intelligence Community (USIC). The request and justification EC must include, depending on the situation:

- (U//FOUO) Reason(s) why the use of a less intrusive method, such as an affiliated approach, is not feasible, and why the covert approach using true name will better assist in evaluating the individual's or PCHS's placement, access, suitability, and susceptibility to becoming a CHS, and possible security concerns.
- (U//FOUO) An explanation of the level of sophistication of the PCHS, including the likelihood that the PCHS will be able to independently identify the SA's FBI affiliation, and the risk that such a disclosure would cause to operational equities, if any.
- (U//FOUO) A description of the proposed CHS identification, evaluation, or recruitment strategy, including the SA's plan to transition the relationship to another SA and remove or distance him- or herself from the individual or PCHS. (Note: Multiple handoffs may occur during the evaluation process. The offer of recruitment, however, must be made by an SA who has fully affiliated himself or herself with the FBI.)
- (U//FOUO) The dates of the SA's attendance at an [redacted] or an equivalent, [redacted] approved course.

#### 3.7.2.3.3. (U//FOUO) Approval for Covert Approach Using True Name

(U//FOUO) Prior SSA approval is required for the use of this approach.

#### 3.7.2.3.4. (U//FOUO) Transitioning From the Covert Approach Using True Name to the Affiliated Approach

(U//FOUO) If, at the outset of the approach strategy or during the course of the execution, the SA determines that revealing FBI affiliation is in the best operational interest of the assessment, the SA must address the following items in the approval request EC:

- (U//FOUO) The reason(s) why the SA believes that affiliation, as opposed to transitioning the individual or PCHS to another SA, is operationally sound and will not compromise the PCHS recruitment effort
- (U//FOUO) The SA's plan to affiliate
- (U//FOUO) The SA's level of training
- (U//FOUO) The SSA's comments regarding the SA's ability to successfully affiliate in the particular CHS identification or evaluation and recruitment scenario

#### 3.7.2.3.4.1. (U//FOUO) Approval to Transition From the Covert Approach Using True Name to the Affiliated Approach

(U//FOUO) SAC (non-delegable) approval to affiliate after using the covert approach with true name is required.

### 3.7.2.4. (U//FOUO) Covert Approach

(U//FOUO) The covert approach allows an SA to employ a CHS identification, evaluation, and/or recruitment strategy in which the SA does not reveal his or her true identity and represents, either affirmatively or through denial, that the SA's employment is something other than with the FBI. For a TFO, the approach involves not revealing the TFO's true identity and representing, either affirmatively or through denial, that the TFO's employment is something other than with the parent LE or intelligence agency or the particular FBI investigative entity, such as a JTTF. In order to protect the technique and any FBI-issued AFID, an SA or a TFO using the covert approach must not affiliate by disclosing his or her true identity or actual employment with the FBI or other LE or intelligence agency, but instead must hand off the PCHS to another SA for further evaluation and an affiliated recruitment. An SA or a TFO in covert status may be permitted to affiliate only in extremely rare circumstances and with appropriate approvals (see subsection 3.7.2.4.4., "Transition From Covert to Affiliated Approach").

(U//FOUO) The covert approach entails the use of an FBI-issued AFID; therefore, it requires a well-devised operational plan to protect the technique and use it effectively, while weighing its use against less intrusive investigative methods to achieve the assessment's objective(s). The factors to consider while crafting an operational plan include the level of sophistication of a given PCHS target; the known or presumed reluctance of a PCHS to talk to the FBI, a member of other LE agencies, or the USIC; and the likelihood of extended contact with and/or overhearing by third parties at a any planned meetings with the PCHS.

(U//FOUO) The covert approach used in a Type 5 assessment is not considered to be undercover activity that is subject to the provisions of DIOG subsection 18.6.13. The distinction lies in the authorized purpose of the Type 5 assessment, which is to seek information to identify, evaluate, and recruit individuals as CHSs. By contrast, undercover activity includes the use of a false identity to obtain intelligence or evidence from a subject or other person of interest. Accordingly, the "five meeting" rule applied to UCO is not applicable to Type 5 assessments.

(U//FOUO) Inherent in utilizing the covert approach is not revealing the true purpose of the contact with individuals encountered under a CHS identification plan or with a PCHS (i.e., the purpose of identifying or evaluating the person as a PCHS). Therefore, the SA must ensure that the purported purpose used for contacting the individual or PCHS:

- (U//FOUO) Is plausible.
- (U//FOUO) Would not reasonably be expected to violate the rights or damage the reputation of another person or entity.
- (U//FOUO) Does not imply that adverse legal consequences may follow to the individual or PCHS (or persons close to them) if the individual or PCHS declines to speak with the SA or TFO.

(U//FOUO) Moreover, the covert approach is permitted only if using it is not reasonably expected to adversely affect the rights or damage the reputation of another person (e.g., the PCHS or other third parties) or to have reasonably anticipated adverse legal consequence, and its use must further the objective(s) of the Type 5 assessment.

#### 3.7.2.4.1. (U//FOUO) Covert Approach Requirements

(U//FOUO) Covert approach requirements must be met when an SA plans in advance to use the approach, prior to contacting the individual or PCHS. Covert approach requirements may also be triggered in situations where a CA, while not revealing his or her true identity during contact with a PCHS, finds it necessary to represent, either affirmatively or through denial, that the CA's employment is something other than with the FBI, and where the CA has used or will use an FBI-issued AFID. For a TFO, this means that the TFO, while not revealing his or her true identity during PCHS contact, finds it necessary to represent, either affirmatively or through denial, that the TFO's employment is something other than with the parent LE or intelligence agency or the particular FBI investigative entity, such as a JTTF. The TFO in this case has used or will use an FBI-issued AFID.

(U//FOUO) In either of the above situations, if the SA or TFO intends to continue to make these representations in the next substantive contact (meaning, a contact that is not made for the purpose of or related to scheduling the next meeting), the SA must obtain prior approval through a written request, as set forth in subsection 3.7.2.4.2., below.

(U//FOUO) In addition, in order to use the covert approach, the SA or TFO must have successfully completed an advanced, DI-sponsored HUMINT course (i.e., [redacted] or [redacted]). Successful completion of equivalent HUMINT training provided by other agencies will be considered on a case-by-case basis and approved by the [redacted]. The Central Intelligence Agency's (CIA) [redacted] is considered equivalent training and does not require FBIHQ approval. A request for [redacted] approval of equivalent training must include the name of the agency providing the training, the course name, and the curriculum and length of the course, and it must be sent to attention of the [redacted] for approval.

(U//FOUO) Since use of an AFID is involved, the SA must obtain the AFID in accordance with requirements in the [redacted] or successor PG. Moreover, any AFID utilized during the evaluation and recruitment process must be official, FBI-

recognized, backstopped, or issued documentation that is consistent with the standards set forth in the [redacted] or successor PG.

### 3.7.2.4.2. (U//FOUO) Request to Use the Covert Approach

(U//FOUO) A request to use the covert approach must be submitted via EC (or successor form in Delta) for approval, as detailed below. If the SA anticipates the operational need for the approach before the Type 5 assessment is opened, the request for the approach should be included in the Type 5 assessment opening request. If the need for the covert approach arises later, the request must be made in a separate EC (or successor form in Delta). For example, this circumstance might occur where the SA utilizes a nonaffiliated approach in a pending Type 5 assessment but, during the contact, finds it necessary to utilize AFID and to either affirmatively or through a denial, that the SA's employment is something other than as a LEO or person in a comparable position in the IC. The request must include:

- (U//FOUO) The reason(s) why use of the affiliated or nonaffiliated approaches would not be feasible in that particular CHS identification, evaluation, or recruitment. If the operational need to use an FBI-issued and backstopped AFID arose during the open Type 5 assessment, and the SA found it necessary to represent, either affirmatively or through denial, something other than an affiliation with LE (or IC equivalent), the SA must explain the circumstances that necessitated this use of the covert approach and why future substantive contact(s) by the SA are feasible and operationally consistent with the purpose and objective(s) of the assessment.
- (U//FOUO) An explanation of the proposed CHS identification, evaluation, or recruitment strategy/operational plan for using the covert approach and how using it will assist with further evaluating the individual's or PCHS's placement, access, suitability, susceptibility to becoming a CHS, and possible security concerns. Factors that should be considered and addressed as appropriate include the level of sophistication of a given PCHS target; the known or presumed reluctance of a PCHS to talk to the FBI or a member of another LE or IC agency; and the likelihood of extended contact with and/or overhearing by third parties at any planned meetings with the PCHS.
- (U//FOUO) A description of the SA's plan to transition the relationship to another SA and remove or distance him- or herself from the individual or PCHS. Note: Multiple handoffs may occur during the evaluation process. The offer of recruitment, however, must be made by an SA who has fully affiliated him- or herself with the FBI.
- (U//FOUO) An explanation of how the AFID will be (or was) used during contact with the individual or PCHS, and whether the PCHS will observe or has observed the AFID.
- (U//FOUO) The dates of the SA's attendance at an advanced, DI-sponsored HUMINT course (or a DI-approved training equivalent), as specified in subsection 3.7.2.4.1, "Covert Approach Requirements."
- (U//FOUO) The date of undercover employee (UCE) certification, if received. Although undercover activity is not permitted in an assessment and the covert approach is not considered as such, UCE experience is a relevant factor to consider in the approval process.

### 3.7.2.4.3. (U//FOUO) Approval to Use the Covert Approach

(U//FOUO) Requests to use the covert approach must be approved by the SAC (non-delegable).

#### 3.7.2.4.4. (U//FOUO) Transition From Covert to Affiliated Approach

(U//FOUO) In order to protect the covert approach, especially since an AFID is involved, an SA using the approach is not permitted to affiliate by revealing his or her true identity or employment to the individual or PCHS. Instead, the SA should develop a relationship with the individual or PCHS to successfully ascertain the PCHS' placement, access, suitability, susceptibility, accessibility, and possible operational security concerns, to the point where that relationship can be transitioned to another SA—or SAs, if more than one handoff is deemed operationally feasible—for an eventual affiliated recruitment.

(U//FOUO) A rare exception to the requirement to hand off the PCHS when using the covert approach is if it becomes operationally necessary to do so, and no other viable option exists to successfully recruit the individual or PCHS. This circumstance should rarely arise and, because of the sensitivity associated with the technique, the request must be given heightened scrutiny by the approving official.

(U//FOUO) SAC (non-delegable) approval to affiliate from the covert approach is required. This approval must be sought whether or not the AFID was subsequently presented to the individual or PCHS. The affiliation request EC, directed to the SAC, must address:

- (U//FOUO) The reason(s) why the SA believes that affiliation, as opposed to transitioning the PCHS to another SA, is operationally sound and will not compromise the evaluation or recruitment effort.
- (U//FOUO) The circumstances of the covert approach (AFID) used
- (U//FOUO) The type of AFID.
- (U/F/OUO) Whether the AFID was actually presented to the individual or PCHS and, if so, in what form and manner.
- (U//FOUO) The SA's plan to affiliate.
- (U//FOUO) The SA's level of HUMINT or other relevant operational training.
- (U//FOUO) The SSA's comments regarding the SA's ability to successfully affiliate in the particular CHS identification or evaluation and recruitment scenario.

#### 3.7.2.4.5. (U//FOUO) Approval to Transition From the Covert Approach to the Affiliated Approach

(U//FOUO) SAC (non-delegable) approval is required to affiliate from the covert approach.

#### 3.7.2.4.6. (U) Use of the Covert Approach by IAs on Publicly Accessible Web Sites

(U//FOUO) During a Type 5 assessment, IAs may access publicly accessible Web sites. While accessing these Web sites, an IA need not always affirmatively disclose FBI affiliation or reveal his or her true identity (e.g., use an alias). If registration is required for access to the publicly available Web site, the IA may use the covert approach to provide the minimum amount of information required for registration. Withholding affiliation is permitted only if doing so is not reasonably expected to violate the rights or damage the reputation of another person or to have reasonably anticipated adverse legal consequences.

(U//FOUO) An FO-assigned IA's use of the covert approach while accessing publically available Web sites requires prior ASAC or senior supervisory intelligence analyst (SSIA) approval (non-delegable). Use of the covert approach while accessing such Web sites by an FBIHQ-assigned IA requires prior unit chief (UC) approval (non-delegable). In addition, prior to use, the alias and other associated alias identification information must be approved by the IA's supervisor and a notification of its use provided to the FBIHQ [redacted] for tracking and deconfliction purposes.

(U//FOUO) The request to use the covert approach must be documented by EC or a successor form in Delta. This request may be included in the opening Type 5 assessment EC or a subsequent EC. The EC must include the justification for using the covert approach, including:

- (U//FOUO) The reason(s) why the use of a less intrusive method for obtaining information or conducting the online activity is not feasible.
- (U//FOUO) Details regarding the alias to be used by the IA.
- (U//FOUO) The IA's successfully completed training on the use of misattributable systems, if relevant.
- (U//FOUO) The Type 5 assessment the covert approach will be used to support, if the request is made subsequently to opening the Type 5 assessment.

(U//FOUO) A separate EC is required for each Type 5 assessment in which the covert approach will be used, even if the approved AFID is the same for more than one assessment. For example, if an IA would like to use the name "Jane Doe," e-mail address jdoe@email.com, as an alias in more than one Type 5 assessment, the IA must request approval for use of the covert approach in each of the Type 5 assessments separately. For guidance regarding misattributable Internet access, visit the [redacted]

(U//FOUO) IAs may not interact with anyone online (e.g., by participating in chat rooms, responding to solicitations, or providing feedback). In other words, IAs may only passively observe. Publicly available Web sites may require registration; however, this does not necessarily make them restricted-access Web sites. If anyone in the general public may register and set up a username and password, the Web site is considered publicly available, and therefore, IAs may access it during a Type 5 assessment after obtaining covert approach approvals, as specified above. Furthermore, if a Web site requires the purchase of access, it is considered publicly available if anyone in the general public can purchase access. However, an IA may not access a Web site if it is owned, operated, administered, or run by a subject of the assessment or predicated investigation, as this may be considered undercover activity, which is prohibited during an assessment.

(U//FOUO) IAs may access publicly available social networking Web sites. However, IAs may not provide any additional covert identification information beyond the minimum required for registration (e.g., name, e-mail address, and physical address). Providing additional information (e.g., interests, photos) is more than mere registration and is not permitted for IAs during a Type 5 assessment. If a Web site restricts access to only "friends" or has other access limitations (e.g., only persons from a certain school may register), then it is not considered publicly accessible, and access by IAs is not permitted during a Type 5 assessment. IAs may not initiate or accept "friend" or similar social network contact requests during a Type 5 assessment.

### 3.8. (U) File Reviews

(U//FOUO) The CA's or IA's immediate supervisor must prepare a file review every consecutive 90-day period (and every consecutive 60-day period for CHS matters undertaken by probationary employees). The file review must be documented in an EC (or a successor form in Delta) and maintained in the [redacted] sub-file for a Type 5 assessment in the identification phase or in the [redacted] file for a Type 5 assessment in the evaluation and recruitment phases. In addition to compliance with all DIOG and FBI CHS policies, the points below must be specifically addressed in the file review.

- (U) For an assessment in the identification phase, the file review must address:
  - (U//FOUO) Whether investigative methods have been used properly (see subsection 3.6., "Authorized Investigative Methods in Type 5 Assessments: All Phases").
  - (U//FOUO) Whether the identification plan successfully narrowed the field to a pool of individuals who might have appropriate placement and access.
  - (U//FOUO) Whether reimbursable expenses incurred by an SA, if any, were reasonable and properly authorized (see subsection 3.9.1., "Identification Phase Funding").
  - (U//FOUO) Whether the progress made in the CHS identification initiative justifies its continuation for an additional 90 days (60 days for probationary employees). If continuation is deemed justified, the SIA or SSA must document the rationale for keeping the Type 5 assessment open.
- (U) For an assessment in the evaluation and recruitment phases, the file review must address:
  - (U//FOUO) Whether authorized investigative methods have been used properly.
  - (U//FOUO) Whether reimbursable expenses incurred by an SA, if any, were reasonable and properly authorized.
  - (U//FOUO) Whether a PCHS was tasked to provide information or was paid for his or her services or expenses.
  - (U//FOUO) Whether a PCHS can or should be recruited.
  - (U//FOUO) Whether the Type 5 assessment should continue for an additional 90 days (60 days for probationary employees). If continuation is deemed justified, the SIA or SSA must document the rationale for keeping the Type 5 assessment open.

### 3.9. (U//FOUO) Funding for Type 5 Assessments

(U//FOUO) Funding is available to cover reasonable costs directly supporting the identification, evaluation, and recruitment phases of a Type 5 assessment, as detailed in the subsections that follow. For the identification phase, SAC payment authority is $1,000 for each assessment opened; for the evaluation and recruitment phases, SAC payment authority is $5,000 for each assessment opened. Unlike investigative funding, SAC payment authority for Type 5 assessments is not automatically renewed at the beginning of each fiscal year (FY). FOs, however, may seek additional funding authority, as set forth below.

(U//FOUO) In order to determine the appropriate funding source for Type 5 assessment activities, the following rules apply:

- (U//FOUO) A Type 5 assessment conducted by a HUMINT squad that supports a positive foreign intelligence (PFI) investigation must utilize HUMINT program funding.
- (U//FOUO) A Type 5 assessment conducted by a HUMINT squad that supports a predicated investigation must utilize appropriate substantive program funding.
- (U//FOUO) A Type 5 assessment conducted by a substantive squad in support of an assessment or predicated investigation must utilize appropriate substantive program funding.

### 3.9.1. (U) Identification Phase Funding

(U//FOUO) In the identification phase, appropriate expenditures may include the SA's travel and fees associated with an event or conference at which an SA expects to identify individuals with placement and access. With prior ASAC approval, light refreshments for a group of individuals in this phase may be approved for up to $100 per event or gathering. This $100 limit does not include expenses attributable to the SA (such as meals and incidental expenses [M&IE] and other miscellaneous expenses) which directly support the CHS identification effort.

(U//FOUO) If a PCHS is identified during the identification phase, identification phase funding will not cover meal and entertainment expenses associated with the SA's evaluation and recruitment activities. In order for that funding to be made available, as discussed in subsection 3.3., "Identification Phase," a separate Type 5 assessment in the evaluation and recruitment phases must first be opened.

(U//FOUO) As noted in subsection 3.9., "Funding for Type 5 Assessments," SAC payment authority in the identification phase is $1,000 for each assessment opened. ASAC approval is required for expenditures up to or equal to $1,000. Requests for enhanced payment authority exceeding $1,000 for any identification initiative must also be approved by the ASAC. If the enhancement request is for a Type 5 assessment that is conducted by an operational squad or supports a predicated investigation other than a PFI, the enhancement request must be sent, via EC, to the appropriate FBIHQ operational unit. If the enhancement request is for a Type 5 assessment conducted by a HUMINT squad that supports an assessment or a PFI investigation, the request must be sent, via EC, to the appropriate [redacted] unit.

### 3.9.2. (U) Evaluation and Recruitment Phase Funding

(U//FOUO) Once a Type 5 assessment is opened on a particular individual in the evaluation or recruitment phase, funding may be used to cover reasonable expenses the SA has incurred in direct support of the evaluation or recruitment of the PCHS. This funding may also include reasonable travel expenses incurred by the PCHS to meet with an SA in furtherance of the recruitment. Funding may not, however, be used to reimburse a PCHS for any expenses not related to travel expenses or to make service payments to PCHSs. Such payments are appropriate only after the PCHS has been opened in Delta, admonished, and is responsive to tasking as a fully opened, operational CHS.

(U//FOUO) As noted in subsection 3.9., "Funding for Type 5 Assessments," SAC payment authority may not exceed $5,000 per assessment. With ASAC approval, the FO may seek additional payment authority. If the enhancement request is for a Type 5 assessment that is

conducted by an operational squad or supports a predicated investigation other than a PFI, the enhancement request must be sent to the appropriate FBIHQ operational unit. If the enhancement request is for a Type 5 assessment conducted by a HUMINT squad that supports an assessment or a PFI investigation, the request must be sent to the appropriate [redacted] unit.

(U//FOUO) Generally, expenses in the evaluation and recruitment phases will be for meals and entertainment incurred in the recruitment of a particular individual. If it is not feasible to obtain an advance of funds to cover these expenses, the SA may pay up to $100 during the Type 5 assessment prior to submitting the draft request. The draft request must be submitted within five calendar days when the $100 limit is reached.

(U//FOUO) When an SA pays for a meal in the course of recruiting a PCHS, the full cost of the meal may be covered, provided that the expense is reasonable under the circumstances. Government per diem rates may be used as a guide for reasonableness but are not determinative. Expenses for the SA's meal must comport with government per diem rates. ASAC approval is required in order for the SA to exceed the government per diem amounts.

(U//FOUO) A gift to a PCHS may also be allowed if it is deemed operationally appropriate. The gift may not exceed $50 and requires SAC approval. The acceptance of gifts by an SA from a PCHS is governed by subsection 2.3.1., "Gifts."

### 3.9.2.1. (U) Evaluation and Recruitment Phase Funding Requests

(U//FOUO) SAs and SSAs must use discretion and exercise fiscal responsibility in determining what type of activity is appropriate in a particular recruitment scenario. In determining whether a particular expense is an appropriate use of resources and is operationally sound and effective, the requesting EC must address:

- (U//FOUO) Whether the SA is using the affiliated, nonaffiliated, covert using true name, or covert approach.
- (U//FOUO) The impact that the expenditure is anticipated to have on the SA's ability to interact effectively with the PCHS. Expenses that do not enhance the SA's ability to evaluate and develop a relationship with the PCHS should not be approved.

(U//FOUO) Each request for funds must receive prior ASAC approval. The EC request must also reference the assessment or predicated investigation used to support the opening of the Type 5 assessment (evaluation and recruitment phases), or the threat program and CPI code(s) the PCHS may support upon successful recruitment.

## 3.10. (U//FOUO) Duration and Closure of a Type 5 Assessment

(U//FOUO) The effective date of a Type 5 assessment is the date on which the highest level of authority required approves the opening EC (or successor form in Delta). A Type 5 assessment may continue for as long as necessary to achieve its authorized purpose and clearly defined objective(s), as set forth in the three phases above, or when it is determined that the named subject cannot or should not be recruited as a CHS.

(U//FOUO) When closing Type 5 assessments, the following language must be included in the synopsis section of the closing EC:

- (U//FOUO) Type 5 assessments closed on a specific named individual who is then opened as a CHS in Delta (Note: All documentation related to the successfully recruited

PCHS must be transferred out of Sentinel and placed into the newly opened CHS Delta file):

"The information from this assessment must be maintained in Delta."

- (U//FOUO) All other Type 5 assessments:

"This assessment did not warrant further investigative effort at this time."

(U//FOUO) Any dissemination from a closed Type 5 assessment must be conducted in accordance with dissemination guidance on CHS closed files and consistent with the principles discussed in Section 15, "Disclosure of a Confidential Human Source's Identity."

### 3.10.1. (U) File Maintenance and Disposition

(U//FOUO) Inasmuch as Delta is the official recordkeeping system for FBI CHS records, all CHS-related documentation must be filed in Delta unless specified otherwise (see Section 16, "Administration of Confidential Human Sources"). However, until Type 5 assessment files can be managed in Delta, open and closed legacy paper files or records serialized into Sentinel must be maintained in the CFR or safeguarded as "prohibited" files in Sentinel. Records relating to PCHSs that are in the identification, evaluation, and recruitment phases are filed into the file classification [redacted] or the [redacted].

(U) The disposition of closed Type 5 assessment legacy paper files is as follows:

- (U//FOUO) Files for Type 5 assessments in the identification phase must be destroyed five years after the file is closed.
- (U//FOUO) Files for Type 5 assessments in the evaluation and recruitment phases must be destroyed five years after the file is closed. The approved disposition authority for records filed under classification [redacted] is [redacted].
- (U//FOUO) Once a PCHS has been successfully recruited and his or her records have been imaged, verified as complete and accurate, and placed in Delta under a unique source number, all hardcopy records related to the CHS filed under the [redacted] may be destroyed. Records related to a PCHS that are created in Sentinel are not authorized for disposal at this time and must be retained until a disposition schedule is approved for these records.

# 4. (U) Opening and Reopening a Confidential Human Source

## 4.1. (U) Use of the CHS Program

(U) The AGG-CHS define a CHS as:

> (U) Any individual who is believed to be providing useful and credible information to the FBI for any authorized information collection activity, and from whom the FBI expects or intends to obtain additional useful and credible information in the future, and whose identity, information, or relationship with the FBI warrants confidential handling.

(U//FOUO) Use of the CHS program should comport with this definition and be based on the following criteria:

- (U) The FBI has established a relationship with an individual who is aware that he or she is working with a representative of the FBI, and the FBI intends the relationship to be ongoing.
- (U) The FBI receives valuable information from the individual on a recurring basis in support of an FBI assessment or predicated investigation, whether in response to taskings or as volunteered information.
- (U) The individual's relationship with the FBI creates a need for confidentiality.

(U) An SA must not open an individual as a CHS if there is no logical reason for confidentiality or if the individual holds a position that would normally compel him or her to provide the information. In addition, sworn U.S. LEOs may not be opened as CHSs. The only exception to this rule is that the SAC may approve the operation of a sworn LEO who has agreed to report on matters involving civil rights or public corruption within his or her employing entity. Similarly, crime victims generally should not be opened as CHSs because their use is limited in terms of time and the nature of the assistance they will provide.

## 4.2. (U) When a CHS May Be Tasked

(U//FOUO) A CHS may be tasked to collect information, intelligence, and evidence and/or provide other assistance only when all of the following have been accomplished:

1. (U//FOUO) The opening communication has been approved.
2. (U//FOUO) All requisite approvals, including (if necessary) those from agencies outside the FBI, have been obtained.
3. (U//FOUO) The CHS has been provided the appropriate admonishments regarding the nature and parameters of his or her relationship with the FBI (see Section 5, "Confidential Human Source Admonishments").
4. (U//FOUO) Required approvals for the specific tasking (e.g., otherwise illegal activity [OIA] or consensual monitoring) have been obtained.
5. (U//FOUO) The CHS has met with the co-CA.

## 4.3. (U) Source-Opening Communication

(U//FOUO) Before an SA prepares the source-opening communication, the FO must conduct a universal query to determine whether the individual has already been opened as a CHS in another FO or legal attaché (Legat). In addition, the SA must do a deconfliction search in Delta

to ensure that the individual in question is not currently open in another office or was previously opened as a CHS. This search must be completed and the results noted within the opening communication. FOs are also expected to conduct local queries and more comprehensive searches, as appropriate, and to document the results in the source-opening communication, as set forth below.

(U//FOUO) If the CHS was previously opened, the opening communication must state the reason why the CHS was closed. If the CHS was closed for cause, either by the FBI or another agency, additional approvals and review will be required (see subsection 4.5.1., "Request to Reopen a CHS Previously Closed for Cause," and subsection 18.3., "Future Contact with a Closed CHS"). If the individual was not previously opened, the communication should simply state that the required deconfliction search was completed with negative results.

(U//FOUO) Only an SA (CA or co-CA) may prepare the source-opening communication. A TFO assigned as a co-CA is not permitted to prepare the opening communication. The SSA must review the communication and determine if the individual should be opened as a CHS. If the SSA approves the communication, notification of the opening must be sent to the appropriate [redacted] unit. Other approvals and/or notifications described elsewhere in this PG, such as approvals that must be made by the SAC or by other agencies, may also be required.

(U//FOUO) The Delta source-opening communication must contain:

1. (U//FOUO) The CHS's biographical information, including his or her:
   - (U//FOUO) Full name, any relevant information related to his or her name (e.g., Chinese numeric designators), and any known aliases.
   - (U//FOUO) Date of birth.
   - (U//FOUO) Place of birth.
   - (U//FOUO) Physical description, including sex, race, height, weight, hair color, eye color, scars, marks, tattoos, and any other available information.
   - (U//FOUO) Current residence.
   - (U//FOUO) Contact numbers (e.g., home phone, cell phone, pager).
   - (U//FOUO) Social security number (SSN).
   - (U//FOUO) Driver's license number, state where issued (e.g., Virginia, South Carolina), and date license issued.
   - (U//FOUO) Citizenship.
   - (U//FOUO) Alien status, if applicable (e.g., visitor, student, diplomat).
   - (U//FOUO) Current and prior occupation, employer, work address, phone number, job title, and nature of job, if known.
   - (U//FOUO) Photograph (print or electronic).
2. (U//FOUO) Information on the CHS's previous relationship with the FBI and other LE and intelligence agencies, including:

- (U//FOUO) Whether the person currently has, or previously had, a relationship with any other LE or intelligence agency and, if so, the name of the agency involved. If the person was a CHS who was closed by another agency, reasonable efforts should be made to determine why the CHS was closed, and the SA must document that reason in the opening communication. If the SA ascertains that the person was closed by another agency for a reason that, under FBI policy, would constitute closing for cause, additional approvals and review will be required (see subsection 4.5., "Requirements for Reopening a CHS," and subsection 18.3., "Future Contact With a Closed CHS"). The SA must describe, in the opening communication, the strategy to be used to mitigate any issues posed by operating the CHS.
  - (S//NF) The above strategy may include operational testing, if deemed appropriate.
- (U//FOUO) Whether the CHS was previously opened as a CHS by the FBI. If so, state the reason why the CHS was closed. If the CHS was closed for cause, either by the FBI or another agency, additional approvals and review will be required. (See subsection 4.5., "Requirements for Reopening a CHS," and subsection 18.3., "Future Contact With a Closed CHS.")
- (U//FOUO) Any promises or benefits that have been given to the CHS by the FBI, FPO, or any other prosecuting or LE agency (if known after exercising reasonable efforts), and the terms of such promises or benefits.

3. (U//FOUO) Information related to operating the CHS, including:
   - (U//FOUO) The investigative classification(s) and/or threat on which the person is expected to provide information and the type of information he or she is expected to provide.
   - (U//FOUO) The geographical areas of operation (e.g., countries, states, cities, zip codes) where the CHS could be used.
   - (U//FOUO) The subject or group on whom the CHS is expected to report.
   - (U//FOUO) The CA and co-CA's names. The SA must state whether the co-CA is an SA or a TFO; if the co-CA is a TFO, the opening communication must identify the TFO's agency and indicate whether that agency brought the CHS to the FBI.
   - (U//FOUO) Documentation that the co-CA has met the CHS. If this meeting has not yet occurred when the CHS is opened, it must take place before the CHS is tasked and be documented in the CHS's main file. The meeting may be documented by any communication which evidences the co-CA's presence, such as a CHS reporting document, payment receipt, or admonishments.
   - (U//FOUO) The FO and squad or Legat that will operate the CHS.
   - (U//FOUO) The CHS's payment name (see subsection 16.3., "Payment Name").
   - (U//FOUO) A request for code name, if needed, for double agents (DAs), non-DAs in joint operations, defectors, recruitments-in-place (RIPs), or unusually sensitive CHSs (see subsection 16.4., "Code Name").

- (U//FOUO) The CHS's motivation in providing information. All likely motivations should be listed, including any consideration sought from the government for this assistance and whether the person has a plea agreement with, or is seeking consideration from, any prosecutor's office.
- (U//FOUO) The person's access to the information he or she is expected to provide.
- (U//FOUO) Whether approvals are required pursuant to Section 6, "Confidential Human Sources Requiring Department of Justice Approval for Operation." If so, a lead must be sent to the [redacted] to notify the Human Source Review Committee (HSRC).

4. (U) Items pertaining to the CHS's background, including:
   - (U//FOUO) Whether the CHS has a criminal history, is reasonably believed to be the subject or target of a pending criminal investigation, is under arrest, or has been charged in a pending prosecution.
   - (S//NF) A request for a CIA name trace if the CHS is primarily reporting on national security matters, travels internationally more than five times annually, or is an emigré, a foreign national, a current or former CIA employee, a CIA contractor, or a CIA applicant. If the SA cannot obtain the information with CHSC assistance, a request may be sent to the appropriate [redacted] unit to request the CIA to conduct the name check and notify the FO or Legat of any relevant information obtained.
   - (U) Immigration and Customs Enforcement (ICE) checks for CHS emigrés who are foreign nationals.
   - (U//FOUO) A synopsis of positive search results of Universal Index (UNI) or the replacement system used for cataloguing subjects of FBI investigations. If necessary, include a statement of concurrence (see subsection 16.6, "Positive Records Checks and Concurrence to Operate.")
   - (U//FOUO) A synopsis of positive search results of ELSUR record checks.
   - (U//FOUO) A synopsis of positive search results of the National Crime Information Center (NCIC) and local criminal history checks. If necessary, include a statement of concurrence for the relevant FO or agency (see subsection 16.6, "Positive Records Checks and Concurrence to Operate.")
   - (U//FOUO) Any relationship the person has with any FBI employee (e.g., brother, mother, friend, roommate, business partner).

### 4.4. (U) Additional Background Information and Records Checks

(U//FOUO) The information listed below, if reasonable to obtain, must be documented before the CHS is tasked and updated promptly if it changes.

- (U//FOUO) Past occupations, including employer, work address, phone number, job title, and nature of job, if known.
- (U//FOUO) Language abilities (spoken and written), other than English.
- (U//FOUO) Skills and hobbies (e.g., computer skills).

- (U//FOUO) Religion
- (U//FOUO) E-mail address and online identity
- (U//FOUO) Names of immediate family members (e.g., spouse, mother, father, brothers, sisters, children)
- (U//FOUO) Past residences
- (U//FOUO) Educational level and, if applicable, current student status
- (U//FOUO) Security clearances or other accesses held (The person may disclose that he or she possesses a clearance but may not disclose the level of the clearance.)

(U) The records checks listed below must be made if deemed useful in evaluating the individual's background or anticipated operation. They include:

- (S//NF) DOS records checks to obtain information about foreign nationals who have applied for a U.S. visa or U.S. citizens who have applied for a passport. If the information cannot be obtained locally, a request may be submitted to the Washington Field Office (WFO). This request should include identifying information about the queried CHS.
- (U//FOUO) Requests to Legats for background checks for CHSs who have foreign citizenship or who have spent a substantial amount of time in a foreign country, if information can be obtained without compromising the CHS's relationship with the FBI. A name check for a CHS who is a foreign government official or employee will almost certainly result in the CHS's compromise. The Legat should be consulted to determine what information may be available without notification to the host country.
- (U//FOUO) Other database inquires (e.g., Financial Crimes Enforcement Network [FinCEN], Lexus Nexus, Treasury Enforcement Communications System [TECS]).

### 4.5. (U) Requirements for Reopening a CHS

(U//FOUO) In order to reopen a CHS who was previously closed, the SA must generate a source reopening communication, which must:

- (U//FOUO) Assign the CHS his or her previous "S" (symbol) number in Delta. If the CHS was previously opened prior to the implementation of Delta, the CHS must be opened in Delta, citing the file number from the legacy file.
- (U//FOUO) Satisfy the requirements of subsection 4.3., "Source-Opening Communication."
- (U//FOUO) Indicate that the CHS is being reopened and provide the reason why he or she was previously closed. If the CHS was ever closed for cause during any prior period of operation, then both the reopening procedures and approvals set forth in subsection 4.5.1., "Request to Reopen a CHS Previously Closed for Cause," and the provisions in subsection 18.1.2., "Closing a CHS for Cause," apply.

(U//FOUO) The approval levels for reopening a CHS are the same as those for opening a CHS for the first time, unless the CHS's status has changed so as to require additional approval (see Section 6, "Confidential Human Sources Requiring Department of Justice Approval for Operation," and Section 7, "Confidential Human Sources Requiring Additional Approvals").

and/or the CHS was closed for cause during any period of operation. If the CHS was previously closed for cause, the approvals set forth in subsection 4.5.1., "Request to Reopen a CHS Previously Closed for Cause," apply.

### 4.5.1. (U) Request to Reopen a CHS Previously Closed for Cause

(U//FOUO) Before initiating contact with or responding to contact from a CHS previously closed for cause, SSA approval must be obtained in accordance with subsection 18.3., "Future Contact With a Closed CHSs."

(U//FOUO) A request to open a CHS previously closed for cause must include the information described in subsection 4.5., above. After stating that the CHS was closed for cause and the reason why he or she was closed, the following additional information must be provided:

- (U//FOUO) The date on which the CHS was closed for cause or, if the CHS was closed for cause on more than one occasion, the date of each such closure
- (U//FOUO) Details supporting each decision to close the CHS for cause
- (U//FOUO) Details regarding the anticipated use of the CHS if reopening is approved
- (U//FOUO) The reason why the use of a different CHS and/or investigative techniques would not be as effective as the CHS in achieving the objectives for the case
- (U//FOUO) Controls that will be placed on the use of the CHS to minimize the risk of harm to others or to the investigation

(S//NF) A request to reopen a CHS previously closed for cause must be approved by the SAC (nondelegable) and by the AD, DI, (nondelegable), whose decision must include a finding as to whether the benefits of reopening the CHS outweigh the risks of reopening the individual. After AD approval has been granted, operational testing requirements must be conducted by the CA in accordance with Section 20., "Confidential Human Source Validation."

### 4.5.2. (U) Closed CHS Reopened by Another Field Office

(U//FOUO) When a closed CHS from one FO is reopened in another FO, the previous FO CHSC must furnish to the new FO CHSC copies of any documents in the file that are not available through Delta. A copy of the entire file must be sent to the new FO CHSC upon request. In addition, the new OO CHSC must promptly be provided with any information that reflects negatively upon the reliability of the CHS.

admonishments have been provided and that the CHS acknowledged receipt and understanding of the admonishments.

(U//FOUO) The content and meaning of the following admonishments must be clearly conveyed:

- (U//FOUO) The FBI on its own cannot promise or agree to any immunity from prosecution or other consideration by an FPO, a state or local prosecutor, or a court in exchange for the CHS's cooperation, because the decision to confer any such benefit lies within the exclusive discretion of the prosecutor and the court. However, the FBI will consider (but not necessarily act upon) advising the appropriate prosecutor of the nature and extent of the CHS's assistance to the FBI. (This instruction should be given if there is any apparent issue of criminal liability or penalty.)
- (U//FOUO) Unless specifically authorized by the FBI, the CHS is not authorized to engage in any criminal activity and has no immunity from prosecution for any unauthorized criminal activity. (This instruction is not necessary for CHSs who have such authorization. The instruction should be given if the CHS is suspected of committing unauthorized illegal activity [UIA]. See Section 12, "Confidential Human Source Participation in Unauthorized Illegal Activity," and Section 13, "Confidential Human Source Participation in Otherwise Illegal Activity.")
- (U//FOUO) The CHS is not an employee of the USG and may not represent him- or herself as such, except under circumstances where the CHS has previously been, and continues to be, otherwise employed by the USG.
- (U//FOUO) The CHS may not enter into any contract or incur any obligation on behalf of the USG, except as specifically instructed and approved by the FBI or under circumstances where the CHS is otherwise authorized to enter into a contract or incur an obligation on the behalf of the United States.
- (U//FOUO) No promises or commitments can be made, except by the Department of Homeland Security (DHS), regarding the immigration status of any person or the right of any person to enter or remain in the United States. (This instruction should be provided if there is any apparent issue of immigration status that relates to the CHS.)
- (U//FOUO) The FBI cannot guarantee any rewards, payments, or other compensation to the CHS.

### 5.3.1. (U) Subjects Represented by Counsel or Planning Legal Defense

(U//FOUO) For additional admonishments related to CHSs who are in a position to obtain information about a subject's pending charges or legal defense plans, see subsection 10.7, "Obtaining Information About a Subject's Pending Charges or Legal Defense Plans."

### 5.3.2. (U) Employees of Financial Institutions

(U//FOUO) These individuals must be advised that they remain subject to the provisions of the Right to Financial Privacy Act and must be advised that the FBI will not knowingly accept information that violates the provisions of the act. This advisement must be documented in the CHS's file.

### 5.3.3. (U) Employees of Educational Institutions

(U//FOUO) These individuals must be advised that they remain subject to the provisions of the Family Educational Rights and Privacy Act of 1974 (Title 20 United States Code [U.S.C.] Section [§] 1232[g]), commonly known as the Buckley Amendment. This statute generally prohibits educational institutions and their employees from releasing non-directory information from records that they maintain on individuals who attend or have attended the institution. There are some exceptions in the statute. For example, Buckley does not apply to a campus police record about criminal activity. Advising the CHS of the provisions of the law is not required if the information the CHS is providing is unrelated to his or her employment. This advisement must be documented in the CHS's file.

### 5.3.4. (U) Otherwise Illegal Activity

(U//FOUO) For additional admonishments related to CHSs who have been approved to engage in OIA, see subsection 13.5., "Admonishments Related to OIA."

# 6. (U//FOUO) Confidential Human Sources Requiring Department of Justice Approval for Operation

## 6.1. (U) Types of CHS That Require DOJ Approval

(U//FOUO) The CHS opening communication must be completed and approved by an SSA. This triggers the [redacted] coordination with DOJ pursuant to subsection 6.2., "*DOJ Review Procedure for CHSs Requiring DOJ Approval*." During the DOJ review and approval process, the CHS may be operated in accordance with this PG.

### 6.1.1. (U) Senior Leadership CHSs

(U//FOUO) The AGG-CHS definition of a senior leadership CHS is as follows:

> (U//FOUO) A Confidential Human Source who is in a position to exercise significant decision-making authority over, or otherwise manage and direct, the unlawful activities of the participants in a group or organization involved in unlawful activities that are: 1) nationwide or international in scope or 2) deemed to be of high significance to the FBI's criminal investigative priorities, even if the unlawful activities are local or regional in scope. Such organizations shall include, but are not limited to: any La Cosa Nostra Family, Eurasian Organized Crime Group, or Asian Criminal Enterprise which is recognized by FBI Headquarters; and any domestic or international Terrorist Organization, which is recognized by FBI Headquarters.

### 6.1.2. (U) High-Level Government CHSs

(U//FOUO) A high-level government CHS is one who is either:

- (U//FOUO) In relation to the federal government or state government of a state, or tribal government, the chief executive or the official next in succession to the chief executive.
- (U//FOUO) A member of the federal, state, or tribal legislature.

### 6.1.3. (U) High-Level Union Official CHSs

(U//FOUO) A high-level union official CHS is one who is a president, secretary-treasurer, or vice president of an international or national labor union or the principal officer or officers of a subordinate regional entity of an international or national labor union. A regional entity does not include a local union or a group of local unions, such as a district council, combined together for the purpose of conducting collective bargaining with employers. See also subsection 7.10., "Union Officials."

### 6.1.4. (U//FOUO) Privileged CHSs

(U//FOUO) A privileged CHS is one who is under the obligation of a legal privilege of confidentiality. State law governs the scope of legal privileges and therefore may vary between jurisdictions. The SA must carefully review each contact with a privileged CHS. If there are questions regarding the protection of privileged information or First, Fifth, and Sixth Amendment rights, the CDC must be consulted.

(U//FOUO) An SA must generally not accept information from a CHS if it relates to privileged communications. However, the use of privileged communications may be permissible in situations involving a potential loss of life, serious physical injury, and destruction of property of substantial value resulting in other serious consequences or contributing to the solution of a

serious crime. If such a situation develops, the SA must notify the CDC and FPO attorney (if one is involved). The CHS's main file must contain thorough documentation of the decision to use privileged information.

#### 6.1.4.1. (U) Attorneys

(U//FOUO) The privilege of confidentiality extends to individuals admitted to practice law and who are engaged in the practice of law. The attorney-client privilege protects certain communications between an attorney and a client. In addition, depending on the facts and the law of the jurisdiction, the privilege may extend to those acting on behalf of the attorney, such as a paralegal. The CDC must be consulted if there are any questions as to whether certain information may be subject to the attorney-client privilege and the extent of the privilege.

#### 6.1.4.2. (U) Physicians

(U//FOUO) The privilege extends to any doctor of medicine (MD) or doctor of osteopathy (DO), and certain jurisdictions may extend the privilege to other medical practitioners. The CDC should be consulted regarding the extent of the privilege in each jurisdiction.

#### 6.1.4.3. (U) Clergy

(U//FOUO) The privilege of confidentiality extends to members of the clergy, as determined by state law. The CDC should be consulted for the extent of the privilege in each jurisdiction.

### 6.1.5. (U) Media CHSs

(U//FOUO) The AGG-CHS define a media CHS as one who is affiliated with the media.

### 6.1.6. (U//FOUO) Long-Term CHSs

(U) A long-term CHS is one who has been open for more than five consecutive years.

(U//FOUO) A CHS not reporting on national security investigations or foreign intelligence collection matters must undergo HSRC review at the five-year mark and every subsequent consecutive five-year period that he or she is open. A CHS reporting on national security investigations or foreign intelligence collection matters must undergo DOJ NSD review at the five-year mark and every subsequent consecutive five-year period that he or she is open. See subsection 6.2., "DOJ Review Procedure for CHSs Requiring DOJ Approval," for more detailed guidance regarding the HSRC and NSD approval processes.

(U//FOUO) All long-term CHSs are subject to the approval requirements in subsection 6.2. The continued handling of a long-term CHS by the same CA for five consecutive years and every five consecutive years thereafter requires SAC approval. This approval may not be delegated, and the SAC may only approve continued handling by the CA for good cause. The SAC approval for continued assignment of the CA to the long-term CHS must be documented prior to submission, detailed in subsection 6.2.

(U//FOUO) The SAC may consider the following factors to determine whether "good cause" exists to continue the CA assignment:

- (U//FOUO) Whether the CA has a unique role in an investigation supported by the CHS, to the extent that the investigation may face impediments due to reassignment of the CA

- (U//FOUO) Whether reassignment of the CA would diminish the FBI's ability to obtain information in a reliable manner due to the sophistication or technical nature of the CHS reporting and the knowledge base of the CA
- (U//FOUO) Whether there are other circumstances that affect the effective operation of the CHS, including the availability of other agents with the requisite experience or capability to operate the CHS

(U//FOUO) ASAC approval is required for the assignment of a probationary SA to operate a long-term CHS as the CA. This approval may not be delegated.

### 6.2. (U) DOJ Review Procedure for CHSs Requiring DOJ Approval

(U//FOUO) DOJ approval is required for the continued operation of any CHS who falls into the categories listed in subsections 6.1.1. through 6.1.5., unless the FPO attorney has existing oversight of the CHS because the CHS has agreed to testify in a federal criminal prosecution. See AGG-CHS, paragraph I (B)(2) for the definition of FPO. DOJ approval is required for all long-term CHSs, as defined in subsection 6.1.6., regardless of whether an FPO attorney has existing oversight of the CHS. The process for obtaining DOJ approval is different for CHSs reporting on national security or foreign intelligence and CHSs reporting on criminal matters.

#### 6.2.1. (U) CHSs Reporting on National Security and Foreign Intelligence

(U//FOUO) DOJ, NSD must approve the continued operation of all CHSs requiring DOJ approval who are reporting on national security investigations or foreign intelligence collection, except as provided in subsection 6.2., above.

(U//FOUO) Upon opening, the CA or co-CA must document the CHS's status as a CHS requiring DOJ approval in the source-opening communication and document the status in the Field Office Annual Source Report (FOASR). The CA or co-CA must also complete and submit the DI's [redacted]. The form may be submitted in Delta to the appropriate [redacted]. In accordance with subsection 20.7.2.2., "Enhanced Review," the CHSs must receive an enhanced review by the appropriate [redacted].

(U//FOUO) If the [redacted] approves the continued operation of the CHS, the [redacted] must provide notice of that approval to DOJ, NSD within 60 days of the approval. The [redacted] must make the CHS's validation reports available for review by the NSD attorney at FBIHQ upon request. If the validation reports do not permit the NSD attorney to conduct a meaningful analysis of the continued use of the CHS, the NSD attorney may ask for additional details. The identity of the CHS must not be disclosed unless the AD or the DAD of the FBIHQ division utilizing the CHS determines that compelling reasons exist to warrant such disclosure. The AD or DAD must consult with the SAC of the FO operating the CHS to determine whether compelling reasons to warrant disclosure exist. With the exception of a request for the identity of a CHS, all requests by NSD for further information pertaining to a CHS must be satisfied within a reasonable period of time. Failure to provide requested information may be grounds for the NSD to recommend that the DAG disapprove the continued use of the CHS. The FBI may continue to operate the CHS pending the resolution of the matter. For additional information about DOJ reviews and the further appeals process, see the AGG-CHS, paragraph II (A)(3)(f).

(U) If a previously opened CHS has a change of status that requires DOJ approval, the CA or co-CA must complete and submit the CHS's status as a CHS requiring DOJ approval on the [redacted] and document the CHS's status in the FOASR.

(U//FOUO) See subsection 20.7.2.3., "Periodic Validation Review," for additional guidance on CHSs reporting on national security and foreign intelligence collection matters.

### 6.2.2. (U) CHSs Not Reporting on National Security Investigations or Foreign Intelligence Collection

(U) The HSRC, which is composed of DOJ and FBI representatives, must approve the continued operation of all CHSs requiring DOJ approval who are not reporting on national security investigations or foreign intelligence collection, except for as provided in subsection 6.2., "DOJ Review Procedure for CHSs Requiring DOJ Approval." Upon opening, the CA must document the CHS's status as a CHS requiring DOJ approval in the source-opening communication and document the status in the FOASR. The CA or co-CA must also complete and submit the DI's [redacted] and the HSRC questionnaire. The [redacted] form may be submitted to the appropriate [redacted] using Delta. In accordance with subsection 20.7.2.2., "Enhanced Review," the CHS must receive an enhanced review by the [redacted].

(U//FOUO) If a previously opened CHS has a change of status that requires DOJ approval, the CA or co-CA complete and submit the Enhanced Review Request form and the HSRC questionnaire. The CA or co-CA must also document the change of status in the FOASR.

(U//FOUO) The appropriate [redacted] unit must seek HRSC written approval for the continued operation of a CHS who falls within the definitions in subsections 6.1.1. through 6.1.5. within 60 days of the CHS's opening. In the case of long-term CHSs, as defined by sub-section 6.1.6, the appropriate [redacted] unit must seek written approval for the continued operation of the CHS upon completion of the enhanced review. The [redacted] must provide to the HSRC relevant information concerning the use of the CHS, including any annual validation reports. The CHS's identity, however, must not be disclosed, unless the FBI chairperson of the HSRC determines that compelling reasons exist to warrant such a disclosure. The HSRC approval process must be completed no later than 45 days after the appropriate [redacted] unit has submitted the request for continued operation of the CHS. The CHS may continue to be operated during the HSRC review process.

# 7. (U//FOUO) Confidential Human Sources Requiring Additional Approvals

(U//FOUO) The CHSs listed in this section have characteristics that require higher levels of approval.

## 7.1. (U) Federal Probationers, Parolees, and Supervised Releasees

(U//FOUO) If an FPO is participating in an investigation in which the FBI seeks to operate a CHS who is a federal probationer, parolee, or supervised releasee, the SA must notify the FPO assigned to the matter and document the notification in the opening communication.

(U//FOUO) Before a federal probationer, parolee, or supervised releasee may be used as a CHS, the CA must obtain the permission of a federal probation, parole, or supervised release official with authority to grant such permission. This permission must be documented in the CHS's main file. If permission is granted, the SSA may approve the opening communication.

(U//FOUO) If permission to use a CHS is denied by the federal probation, parole, or supervised release official, or if it is inappropriate, for operational reasons, to seek permission from the appropriate official, the ASAC (non-delegable) may authorize the CA to request approval for operation of the CHS from the court responsible for the CHS's probation, parole, or supervised release after consulting with the FPO for that district.

## 7.2. (U) Prisoners Under Bureau of Prisons (BOP) Supervision or in the Custody of the United States Marshals Service (USMS)

(U//FOUO) The approvals and procedures addressed in this subsection apply not only to federal prisoners managed by the BOP, but also to state and local prisoners housed in a BOP facility, and to any prisoners housed in a state or local facility who are under BOP supervision or in USMS custody.

### 7.2.1. (U) FPO, BOP, and USMS Approval

(U//FOUO) The opening communication must document the notification to the FPO attorney assigned to the matter in which the CHS will assist. It must also document the permission obtained by the FO from the appropriate authority in the BOP or USMS, as follows:

- (U//FOUO) If the CHS is housed in a BOP institution, the appropriate authority is the warden.
- (U//FOUO) If the CHS is housed in a BOP halfway house, is under BOP home detention, or is being monitored electronically by BOP, the appropriate authority is the BOP community corrections manager.
- (U//FOUO) If the CHS is in USMS custody and is housed in a state or local facility, the appropriate approving official is the highest-ranking USMS official in that district.

(U//FOUO) If permission is denied or it is inappropriate, for operational reasons, to contact the appropriate BOP or USMS official, the CHS opening communication must document the reason why the approval was denied or not sought.

(U//FOUO) Upon completion of the above, the CA must follow the coordination and approval procedures set forth in DIOG Appendix C. This process involves consultation with the FBIHQ

operational unit and the appropriate [redacted] unit and approval of the CHS's operational use by DOJ's Office of Enforcement Operations (OEO).

### 7.3. (U) State or Local Prisoners, Probationers, Parolees, and Supervised Releasees

(U//FOUO) Prior to opening a state or local prisoner, probationer, parolee, or supervised releasee as a CHS, the SSA must determine whether utilizing that person in this capacity would violate the terms and conditions of the person's incarceration, probation, parole, or supervised release. If the SSA has reason to believe that utilizing the individual as a CHS would violate these terms and conditions, the SSA (or his or her designee, who may be the CA) must obtain—prior to operating the person as a CHS—the permission of a state or local prison, probation, parole, or supervised release official with authority to grant permission. This authorization must be documented in the CHS's file.

(U//FOUO) If permission is denied or it is inappropriate, for operational reasons, to contact the appropriate state or local official, the SSA (or designee) may seek authorization to use the individual as a CHS from the state or local court then responsible for the individual's incarceration, probation, parole, or supervised release. If permission is granted, an SSA may approve the opening of the CHS.

(U//FOUO) It should be noted that the use of a state or local probationer, parolee, or supervised releasee as a CHS will likely violate the conditions of his or her status.

(U//FOUO) If an FPO is participating in an investigation using the CHS or would be working with the CHS in connection with a prosecution, the CA must notify the FPO attorney assigned to the matter prior to opening the CHS and must document the notification in the CHS opening communication.

#### 7.3.1. (U) Approval to Release a State or Local Prisoner From Custody

(U//FOUO) A request for the temporary or permanent release of a sentenced state or local prisoner from custody to assist the FBI requires approval from the SAC and the appropriate prison official or court. If an FPO is participating in an investigation using the CHS or would be working with the CHS in connection with a prosecution, the CA must notify the FPO attorney assigned to the matter prior to using the CHS.

(U//FOUO) The criteria that must be addressed in the request to the SAC include:

- (U//FOUO) The length of time remaining on the prisoner's sentence.
- (U//FOUO) The significance of the investigation for which the prisoner's release is being sought and the importance of the prisoner's assistance to that investigation.
- (U//FOUO) The prisoner's criminal history—in particular, whether there is any history of violent crime—and his or her disciplinary record during the period of incarceration.
- (U//FOUO) Whether there are known, identifiable, or potential victims of the prisoner, including trial witnesses against him or her or others against whom the prisoner has made threats and, if so, whether warning those individuals is likely to compromise the investigation in which the prisoner is expected to participate. (Notifying known, identifiable, or potential victims that the prisoner will be released may be required unless it is likely to compromise the investigation. Consult the FO's victim/witness coordinator.)

- (U//FOUO) Confirmation that precautions will be taken to ensure that the prisoner remains in the constant custody of the FBI or under FBI surveillance during the entirety of the prisoner's release. The SAC must adequately resource the mission during the entirety of the CHS's release.

### 7.4. (U) BOP Personnel

(U//FOUO) A request to operate a BOP employee to assist in investigative activity or provide information pertaining to a subject in a BOP facility requires OEO approval. However, OEO approval is not required to conduct routine interviews of BOP personnel or to open a BOP employee as a CHS to report on matters unrelated to his or her work with the BOP.

(U//FOUO) When OEO approval to use a BOP employee as a CHS is required, the CA must prepare a letterhead memorandum (LHM) request suitable for dissemination, with a cover EC, that must be approved by the SSA and then sent with an action lead to the appropriate [redacted] unit. The [redacted] unit must then coordinate with the appropriate operational unit, forward the request to the OEO, and notify the FO of the OEO's decision. The LHM request must include:

- (U//FOUO) The name of the BOP employee.
- (U//FOUO) The location and job title of the BOP employee.
- (U//FOUO) A description of the necessity of using the BOP employee in the investigation, including alternative investigative techniques that have been tried or considered and why these techniques have not worked or have not been tried. The request must detail the activity in which the employee is to be engaged and the location and length of time the employee would be needed. Specifically, the request must state whether the employee would be required to contact subject(s) or the relatives, friends, or associates of subjects outside of the institution in connection with this investigation.
- (U//FOUO) The name of each subject of the investigation and his or her role in the crime(s) or organization under investigation.
- (U//FOUO) The security measures to be taken to ensure the BOP employee's safety.
- (U//FOUO) The name of the concurring FPO attorney if the CHS is likely to testify.
- (U//FOUO) Whether a job transfer of the BOP employee will be necessary upon completion of the activity.
- (U//FOUO) The way in which the activity jeopardizes the BOP employee's family, if applicable.
- (U//FOUO) The name, phone number, title, and location of any BOP employee with whom the matter has been or will need to be discussed.

### 7.5. (U) State, Local, or Contract Prison Employees

(U//FOUO) SSA approval is required to open state or local prison employees or individuals contracted with state or local prisons as CHSs. However, individuals in this category who are sworn LEOs must be opened in accordance with subsection 7.6., below.

### 7.6. (U) Sworn Law Enforcement Officers

(U//FOUO) Every U.S. LEO, regardless of his or her particular assignment, has an ethical and professional responsibility to report criminal activity or matters affecting national security. Therefore, no U.S. LEO may be opened as a CHS. The only exception to this rule is that the SAC may approve the operation of a sworn LEO who has agreed to report on matters involving civil rights or public corruption within the LEO's employing entity.

(U//FOUO) This policy extends to sworn U.S. LEOs employed in the police departments of universities and other academic institutions.

### 7.7. (U) Employees of Federal, State, Local, or Tribal Agencies

(U//FOUO) If an employee of a federal, state, local, or tribal agency has a duty to share information with LE as part of the terms of his or her employment, the individual should not be opened as a CHS. An exception to this rule is that the SAC may approve operation of an employee of a federal, state, local, or tribal agency who has agreed to report on matters involving civil rights or public corruption within the individual's employing entity.

### 7.8. (U) Minors (Individuals Under the Age of 18)

(U//FOUO) SAC authorization (cannot be delegated) is required to open an individual under the age of 18 as a CHS. The opening communication must indicate:

- (U//FOUO) Whether the minor resides with his or her parents or is legally emancipated, as defined by state law.
- (U//FOUO) If the minor is not emancipated, whether parental or legal guardian consent has been obtained for his or her use as a CHS.
- (U//FOUO) If parental or legal guardian consent has not been obtained, whether consent can or will be obtained. If it is not feasible to obtain consent from the minor's parents or legal guardian, the opening communication must provide the justification for using the minor in the absence of such consent.
- (U//FOUO) The potential risk of harm the proposed operation poses to the minor.
- (U//FOUO) The minor's criminal record, if known.
- (U//FOUO) The minor's relationship, if any, to the subject(s) of the investigation.

(U//FOUO) The CA must consult the CDC if there are questions regarding the criteria for legal emancipation.

(U//FOUO) If the minor is emancipated or the SAC has approved the use of the minor without the consent of his or her parents or legal guardian, any service or expense payments must be made directly to the minor. However, if the parents or legal guardian have provided consent, any service or expense payments must be made to the parents or legal guardian, and they must sign the payment receipt.

### 7.9. (U) Counselors, Employees, and Patients in Substance Abuse Treatment Programs

(U//FOUO) SAC approval (cannot be delegated) is required to open a counselor, employee, or patient in a substance abuse treatment program as a CHS, regardless of the nature of the CHS's reporting. A court order is required before placing a CHS in a substance abuse facility or using

an employee or a patient of a substance abuse treatment facility if the individual is going to provide information on the employees of, or patients in, such a program (see Title 42 Code of Federal Regulations § 2.67). If the individual is being opened to obtain information unrelated to his or her employment, employees, or patients in substance abuse treatment programs, a court order is not required. The type of information the CHS will be tasked to obtain, however, must be documented in the CHS's main file.

### 7.10. (U//FOUO) Union Officials

(U//FOUO) An SSA may approve the opening of a union official as a CHS, though HSRC approval or DOJ review may be required if the official is high-level (see subsection 6.1.3., "High-Level Union Official CHSs," and subsection 6.2., "DOJ Review Procedure for CHSs Requiring DOJ Approval." If a CHS is a union official of any rank, the SA must advise the CHS that the CHS remains subject to the reporting provisions of the Employee Retirement and Income Security Act (ERISA) of 1974, and must not operate in a manner that adversely affects union-affiliated pensions, welfare, and benefits. Union officials are charged with specific duties and obligations under ERISA (e.g., duties related to retirement, benefits, or other income benefits of union members).

### 7.11. (U) Department of Energy (DOE) Personnel

[redacted]

requires the FBI to obtain prior approval from the director of DOE's Office of Counterintelligence prior to using a DOE employee as a CHS in a counterintelligence investigation. A DOE contractor may be considered an employee to the extent that he or she affects DOE interests or activities. The opening request must be approved by the ASAC and forwarded to [redacted] must seek DOE approval and notify the FO of the DOE's decision. The request must contain the DOE employee's:

- (U) Full name.
- (U) Date of birth.
- (U) Place of birth.
- (U) Job title.
- (U) DOE agency of employment.
- (U) Duty location.

(U) The request must also contain:

- (U//FOUO) A description of the investigation and the necessity of CHS's assistance.
- (U//FOUO) A description of the CHS's anticipated activities.

### 7.12. (U) Personnel Affiliated With the Department of Defense (DoD) (Not Including Joint Operations With DoD)

(U//FOUO) The MOU titled, "Coordination of Counterintelligence Matters Between FBI & DOD" (June 20, 1996) requires the FBI to coordinate with the appropriate DoD authority the use of DoD personnel as CHSs in unilateral operations (not joint operations with DoD).

(U//FOUO) The degree of coordination required, as set forth below, will depend upon the position of the individual the FBI wishes to open as a CHS and whether the proposed use of the individual is based upon or related his or her association with DoD.

(U//FOUO) The CDC and/or OGC should be consulted to determine whether the proposed operational use of a military member would risk violating the Posse Comitatus Act, 18 U.S.C. § 1385.

### 7.12.1. (U//FOUO) Definitions

(U) The following definitions apply to this section:

- (U//FOUO) **DoD-affiliated personnel:** DoD active duty and retired personnel, civilian employees, contractors and their employees, active and inactive reservists, National Guard members, family members of active duty and civilian personnel, persons residing on or having official access to DoD facilities, persons under consideration for DoD employment and former DoD employees and contractors.
- (U//FOUO) **Concurrence:** The SA seeking to open a DoD-affiliated person as a CHS must request, via an SAC-approved EC, that the [redacted] seek the input and concurrence of DoD prior to operating the individual as a CHS. The CHS may not be operated until any identified objections by DoD have been resolved.
- (U//FOUO) **Military Department Counterintelligence Organization (MDCO):** Army Counterintelligence (CI), the Naval Criminal Investigative Service (NCIS), and Air Force Office of Special Investigations (AFOSI).

### 7.12.2. (U//FOUO) Concurrence Requirements

(U//FOUO) DoD concurrence is always required for active duty military personnel, reservists on active duty, and DoD civilian employees.

(U//FOUO) For all other DoD-affiliated personnel:

- (U//FOUO) DoD concurrence is required whenever the proposed FBI utilization of the individual as a CHS is connected in some fashion with the individual's DoD affiliation.
- (U//FOUO) DoD concurrence is not required whenever the proposed FBI utilization is not connected in any way with the individual's DoD affiliation. However, if facts arise in the course of operating the CHS that reasonably indicate that the FBI utilization of the individual as a CHS is connected in some fashion with the individual's DoD affiliation, operation of the CHS may not continue until DoD concurrence is obtained.

### 7.12.3. (U//FOUO) Concurrence Procedures

(U//FOUO) The SA must notify the [redacted] of the need for DoD concurrence via an SAC-approved EC setting out the circumstances of the request to operate the DoD-affiliated person as a CHS. The EC must contain the following:

- (U) Full name
- (U) Date of birth
- (U) Place of birth
- (U) SSN

- (U) Rank/grade
- (U) Duty position
- (U) Duty organization
- (U) Duty location
- (U) Duty telephone number
- (U) Information about the subject of the investigation, including the activities of the individual or group and any establishment or other affiliations (e.g., criminal, terrorism, intelligence, and the like)
- (U) The anticipated CHS activities and tasking
- (U) The results of the CHS's completed background investigation
- (U) The FBI POC and his or her phone number
- (U//FOUO) A statement of whether the CHS's military commander is aware of the CHS's cooperation with the FBI (if so, the name of the commander and notification date must be included)

(U//FOUO) The [redacted] must seek concurrence from the appropriate DoD entity as set forth below.

(U//FOUO) When the CHS is affiliated with a military department (e.g., an active duty servicemember, a dependent of an active duty service member, or a contractor assigned in direct support of a military department), the [redacted] must contact the appropriate MDCO for that military department prior to initiating operational use of the individual. The [redacted] must prepare an LHM to the DoD entity that contains:

- (U) The results of FBIHQ indices checks.
- (U) A request for DoD concurrence for the use of the CHS.
- (U//FOUO) A request to be advised whether the appropriate DoD entity wishes to participate in interviews or debriefings of the CHS and, if so, to designate a participant.
- (U//FOUO) A request (if deemed appropriate) that the appropriate DoD entity conduct its own records checks on the CHS (see subsection 7.12.3.1., "Request for DoD Records Check").

(U//FOUO) The [redacted] must advise the CA of the DoD response. The CA must then upload the results and any related documents to the CHS file.

(U//FOUO) When the CHS is affiliated with a defense component that is not itself an entity of a military department (e.g., a civilian employee of a defense agency, a dependent family member of such a civilian employee, or a contractor assigned in direct support of the defense agency), the [redacted] must contact the component's office of counterintelligence and/or security, as applicable. The [redacted] must prepare a cover letter to the DoD entity that contains:

- (U//FOUO) The results of FBIHQ indices checks.
- (U//FOUO) A request (if deemed appropriate) that the appropriate DoD entity conduct its own records checks on the CHS (see subsection 7.12.3.1., below).

(U//FOUO) The [redacted] must advise the CA of the DoD response. The CA must then upload the results and any related documents to the CHS file.

### 7.12.3.1. (U//FOUO) Request for DoD Records Check

(U//FOUO) When submitting requests for concurrence to DoD, the [redacted] may send to the DoD MDCO or component CI or security office an internal record check request (e.g. local and official personnel files) to ascertain the existence of derogatory information on the prospective CHS which might contraindicate usage of that individual as a CHS. All DoD entity records check information provided to the [redacted] must be sent to the requesting SA and must be serialized into the CHS file.

### 7.12.3.2. (U//FOUO) Adjudication Procedures

(U//FOUO) In the event of a disagreement between the [redacted] and DoD regarding operation of the CHS, the [redacted] must make every effort to resolve the disagreement at the lowest level possible, escalating as necessary to achieve satisfactory resolution.

(U//FOUO) In the event that a resolution is not achievable, the [redacted] must notify the AD of the DI, who must communicate with the director or commander of the respective MDCO within five working days of their inability to reach a satisfactory resolution.

(U//FOUO) In the event that the matter is not resolved at the AD level, the matter will be referred within ten working days after impasse to the Under Secretary of Defense for Intelligence and the EAD, Intelligence Branch. The Intelligence Branch EAD has final decision-making authority on the matter, including caveats placed on the DoD affiliated person's operation as a CHS.

## 7.13. (U) Fugitives

(U//FOUO) A fugitive is an individual for whom:

- (U//FOUO) A federal, state, or local LE agency has placed a wanted record in the FBI's NCIC (other than for a nonmoving traffic violation).

OR

- (U//FOUO) A federal warrant has been issued.

AND

- (U//FOUO) An LE agency is willing, if necessary, to seek extradition to its jurisdiction.

(U//FOUO) A known fugitive may not be opened or operated as a CHS, and a CHS who is known to have become a fugitive must be closed.

(U//FOUO) An SA may communicate with a former CHS who is a fugitive only if either:

- (U//FOUO) The communication is approved in advance by the SSA; a supervisor of any federal, state, or local LE agency that has a wanted record for the individual in the NCIC; and the FPO in the issuing district, if the warrant is federal.
- (U//FOUO) The communication is not approved in advance, but was initiated by the fugitive or is part of a legitimate effort to arrest the fugitive or convince the fugitive to turn him- or herself in.

(U//FOUO) An SA who communicates with a fugitive CHS in either of these circumstances must promptly report the communication to the SSA and the appropriate federal, state, or local LE agency that has a "wanted" record for the individual in the NCIC. The SA must document, in the CHS's main file, the communication, the circumstances under which the communication was initiated, approvals that were obtained or a statement that no approvals were obtained, and the entities to whom the communication was reported.

### 7.14. (U) Illegal Aliens

(U//FOUO) See Section 9, "Immigration Matters."

### 7.15. (U) Former FBI Employees and Persons With a Present or Former Relationship With an FBI Employee

(U//FOUO) Prior to opening a former FBI employee or a present or former spouse or significant other of an FBI employee as a CHS, the squad supervisor proposing the opening must present to the SAC and document in the CHS opening communication a detailed justification explaining the reason why this individual requires the protection of the FBI's CHS program, along with the SAC's approval (this approval requirement may not be delegated). All admonishments apply to former FBI employees and the spouses or significant others of FBI employees if they are opened as CHSs.

(U//FOUO) SSA-approved payments to an individual in one of the aforementioned categories are restricted to reimbursements for expenses incurred in direct support of an investigation and relocation expenses, if justified and necessary. Compensation to these individuals for their services as CHSs, including lump-sum payments, must be approved by the SAC (this approval may not be delegated). The CA should consult with the CDC, who may confer with the section chief (SC) of the [redacted] to determine whether a service agreement should be used. If applicable, an FPO attorney participating in the conduct of the investigation must be consulted regarding these payments.

(U//FOUO) Opening a former FBI employee as a CHS in order for that person to continue to contact or operate other CHSs or sub-CHSs is not permitted. Generally, doing so in order for the former FBI employee to work or continue to work in an undercover capacity in an FBI investigation is also not permitted. To determine whether these individuals may work in an undercover capacity, contact the [redacted] at FBIHQ. For more information, see subsection 10.4., "Undercover Operation." [redacted]

### 7.16. (U) Current or Former Participants in the Witness Security Program (WSP)

(U//FOUO) See subsection 8.3., "Use of a Current or Former WSP Participant as a CHS."

### 7.17. (U) Members of Congress and Their Staffs

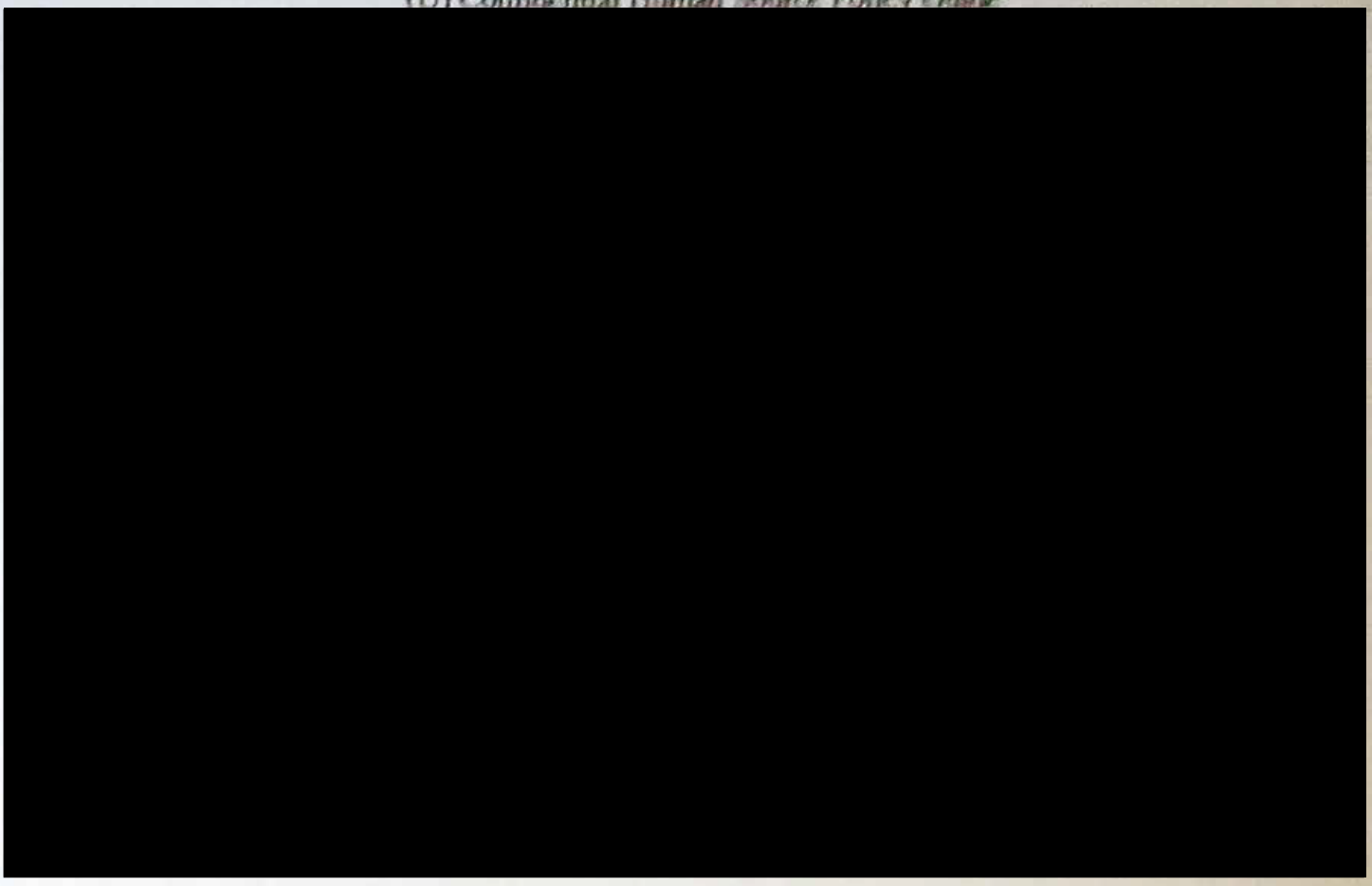
(U//FOUO) A request to open a member of the U.S. Congress or a U.S. Congressional staff member as a CHS requires the following approvals (which may not be delegated) and notifications: SAC and operational division AD approval; operational branch EAD approval; notification to the AD, OCA; and notification to the [redacted] If the CHS is approved, the operational division must consult DOJ's Public Integrity Section (PIN) for guidance regarding the Speech or Debate Clause.

### 7.18. (U) White House Personnel

(U//FOUO) A request to open an employee or member of the White House staff as a CHS requires SAC approval and notification to the operational branch EAD, operational division AD, appropriate operational unit, and [redacted]. If any notified FBIHQ official has questions or concerns regarding the operation of the CHS, he or she should contact the SAC to resolve the issue. The approval may not be delegated.

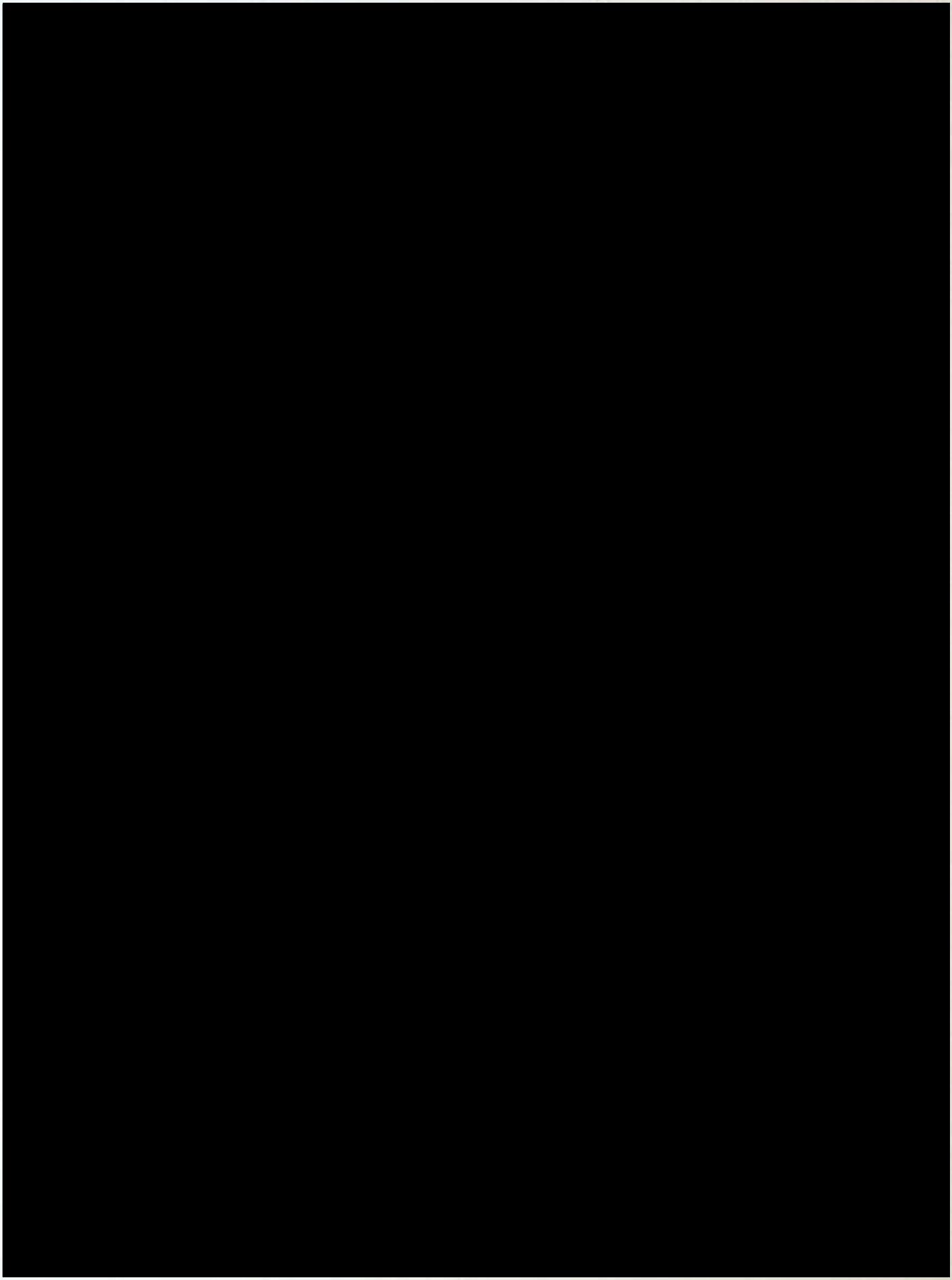
### 7.19. (U) No Foreign Policy Objection Statement

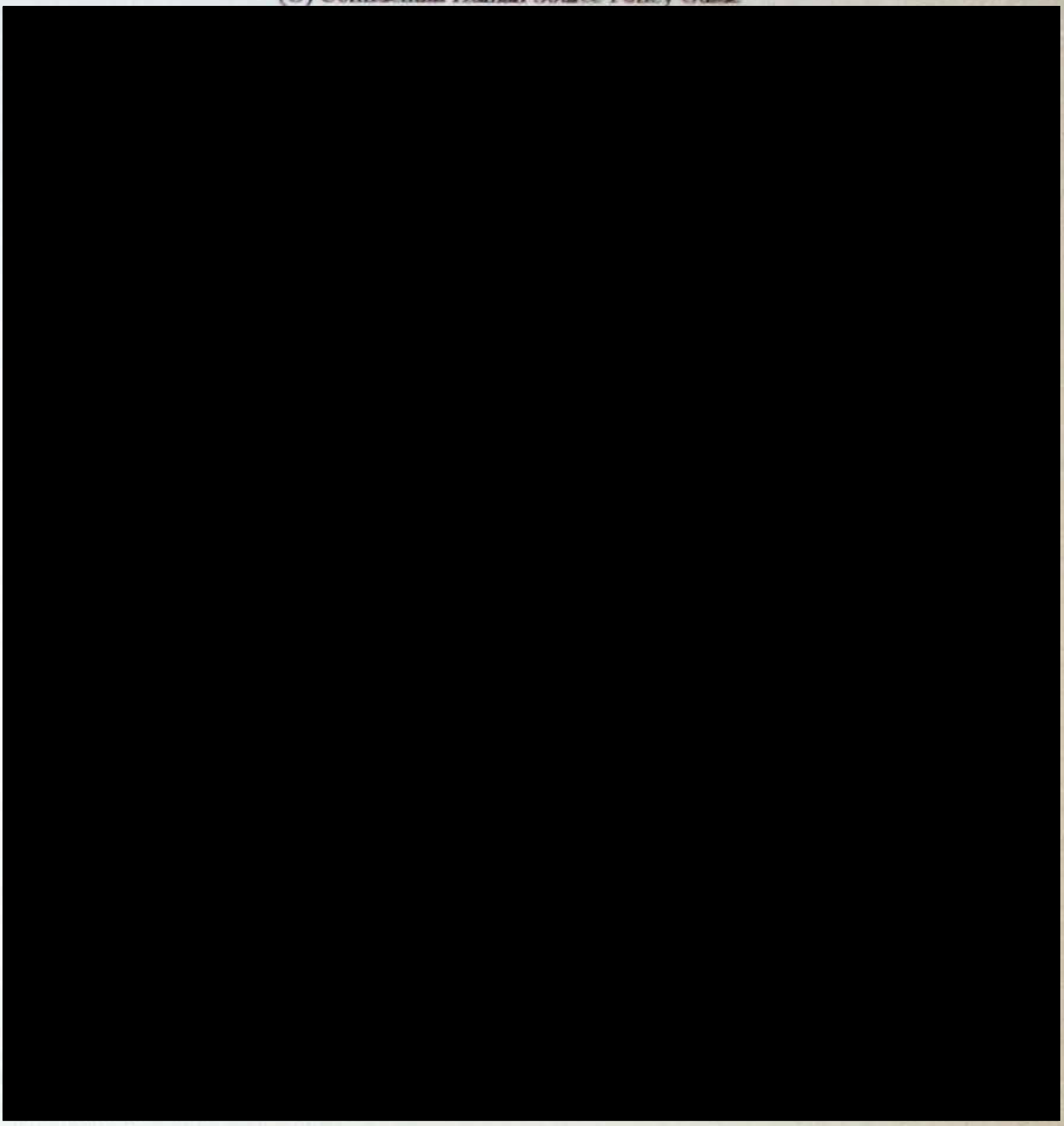
[redacted]



## 8. (U) Witness Security Program

[redacted]





# 9. (U) Immigration Matters

## 9.1. (U//FOUO) CHSs in the United States Illegally

(U//FOUO) The FBI must initiate procedures to legitimize the immigration status of a CHS who is known to be in the United States illegally. This section details the requirements for opening and closing CHSs known to be in the United States illegally and the processes available—from the DHS's ICE and United States Citizenship and Immigration Services (USCIS) and through the CIA—for acquiring legal immigration status for or delaying the deportation of those CHSs.

## 9.2. (U) Requirements for Opening, Operating, and Closing

(U//FOUO) A CA may open and operate an illegal alien as a CHS with SSA approval. However, the CA must request an adjustment of the CHS's status—through one of the procedures set forth in subsection 9.3., below—no more than 90 calendar days after the CA determines that the individual is in the United States illegally. This process also applies to a previously opened CHS who loses his or her legal status. The request for status adjustment must be documented in the CHS's main file.

(U//FOUO) Although an illegal alien may be operated as a CHS while a request to ICE to adjust his or her legal status is pending, the CHS must be closed if ICE denies the request. The CA may request the [redacted] to intercede with ICE headquarters to reconsider the denial, but must not reopen and operate the CHS unless notified by the [redacted] in writing that ICE has agreed to adjust the CHS's immigration status. ICE's decision must be documented in the CHS file.

(U//FOUO) If a determination is made to close the CHS, and if the CA has not requested legal status on behalf of the CHS, then the CA must refer the matter to ICE to coordinate a resolution of the CHS's immigration status (e.g., deportation). If the CA has already initiated a request to obtain legal status on behalf of the CHS, the CA must contact [redacted] which must contact ICE to coordinate the termination of those proceedings.

(U//FOUO) The sponsoring CA is responsible for CHSs who have received legal immigration status. The CA must make reasonable efforts to ensure that these CHSs do not violate any U.S. laws while they are in the United States.

(U//FOUO) If any illegal alien CHS is determined to be unreliable or no longer suitable for use as a CHS, the CA must close him or her and notify the [redacted] in writing of the individual's status and location. The [redacted] must notify ICE headquarters to terminate the CHS's adjustment of status, as appropriate. The CA must also notify the local ICE office of the CHS's status and location. If the CHS's location is unknown, the CA must work with ICE to locate the individual.

## 9.3. (U) Available Programs for Acquiring Legal Immigration Status for a CHS and Delaying a CHS's Deportation

(U//FOUO) Prior to initiating any request to obtain legal status for a CHS, the CA must contact the [redacted] to determine whether the CHS is eligible to obtain legal status and, if so, the best process to employ.

### 9.3.1. (U) Significant Public Benefit Parole Program

(U//FOUO) The Significant Public Benefit Parole (SPBP) is a temporary measure used to support LE efforts by providing a legal mechanism for inadmissible or deportable alien CHSs, witnesses, subjects, and defendants to be present in the United States to assist with ongoing

investigations and prosecutions or engage in other activities necessary to protect national security. The parole allows an inadmissible alien to legally enter or remain in the United States during this period and, upon request, may allow the issuance of work authorization. If the alien is eligible for a visa or a border crossing card (BCC), this option must be considered first before applying for SPBP. The SPBP will not confer any immigration status on the inadmissible alien.

(U//FOUO) The DHS, Homeland Security Investigations (HSI), Law Enforcement Parole Unit (LEPU) (hereafter referred to as ICE) is the authorizing agency for the SPBP and deferred action (see subsection 9.3.2., "Deferred Action Program") programs for all USG agencies and is governed by U.S. Immigration Law, Title 8 Code of Federal Regulations § 212.5, Parole of Aliens into the United States. [redacted] facilitates the coordination between the FBI and ICE to facilitate all SPBP and deferred action applications on behalf of the FBI.

(U//FOUO) To initiate an SPBP request and determine the type of SPBP parole for which the CHS is qualified and the procedures necessary, the CA should review the [redacted] for current application procedures and contact [redacted] with any questions. When determining whether to submit an SPBP request, the CA should be aware that a CHS's criminal record, especially if it includes crimes of violence, may cause ICE to deny a request.

(U//FOUO) An SPBP recipient is the responsibility of the sponsoring FO. The CA must take reasonable measures to ensure that the CHS does not violate any U.S. laws while living in the United States. If the CA reasonably believes that the CHS has engaged in UIA, the CA must notify [redacted] and [redacted] must notify ICE to determine what action must be taken. Furthermore, when the CHS's assistance to the FO has been completed, the CA must notify [redacted] and the local ICE office and, if necessary, work with ICE to locate the CHS. If the CA seeks to obtain legal status for the CHS following his or her assistance, the CA should contact [redacted] to determine the circumstances and criteria that permit this to occur. (See also subsection 9.3.4., "S Visa Program," and subsection 9.3.5., "Public Law 110 Program.")

#### 9.3.1.1. (U) CONUS and OCONUS Eligibility

(U//FOUO) If the alien is not in the United States and is otherwise inadmissible, the applicable immigration program is the SPBP.

(U//FOUO) If the alien is currently in the United States without legal status, SPBP may still apply. Eligibility for SPBP depends on the alien's immigration record and how he or she entered into the United States. If the alien entered without inspection and was never subject to removal (i.e., deportation) proceedings, then the alien is eligible for an SPBP referred to as a "parole in place," under which the alien is not required to leave the country and reenter. The alien will receive his or her I-94 (the form used to track arrivals and departures) from the local ICE office.

(U//FOUO) If the alien is currently in removal proceedings or has ever been previously removed, the agent must apply for deferred action. If the alien was previously legally admitted to the United States, but is now without legal status (i.e., a visitor visa overstay), the agent must apply for deferred action.

(U//FOUO) The alternative to deferred action is to have the alien voluntarily depart the United States and for the agent to apply for SPBP to have the individual paroled back into the country. Upon parole approval, the parole travel documents can be obtained from the ICE representative at the local U.S. consular office, and then the alien can reenter the United States at the port of entry specified in the SPBP application form.

### 9.3.1.2. (U//FOUO) General Considerations

#### 9.3.1.2.1. (U) Control Agent

(U//FOUO) ICE refers to the agent responsible for the alien as the "control agent." For the purposes of this section, the control agent is the CHS CA requesting the SPBP or deferred action and can be changed at any time by notifying [redacted] which will then notify ICE of the change.

(U//FOUO) Under both the SPBP and deferred action programs, it is important for the control agent to understand his or her responsibilities. The CA must take reasonable steps to ensure that the alien is not violating the law. Furthermore, the agent must immediately report any arrest of the alien to [redacted] and coordinate with ICE for his or her removal. The control agent must exercise due diligence to ensure that the alien voluntarily departs the United States or is transferred to ICE custody at the end of the alien's parole or cooperation.

#### 9.3.1.2.2. (U) Multiple Entries

(U//FOUO) A CA should consider whether there is an operational need for the alien to leave the country and reenter. In the SPBP program, an agent may request that the parolee be allowed multiple entries into the United States during the parole period. In the deferred action program, an alien is not eligible for reentry into the United States. If the alien in the United States is not eligible for an SPBP parole in place, but needs multiple entries, the agent should consider applying for SPBP with multiple entries and have the alien voluntarily leave and reenter at a designated port of entry.

#### 9.3.1.2.3. (U) Dependents and Family Members

(U//FOUO) Family members or other dependents (i.e., derivatives) may be paroled only under extraordinary circumstances, such as legitimate physical threats to those individuals. The threats must be clearly documented by the CA in a detailed threat assessment. An example of a threat assessment LHM is located on the [redacted] Multiple entries are not typically granted to family members or dependents of parolees because they are generally paroled on the basis of the threat assessment, and leaving the United States is inconsistent with safety concerns.

(U//FOUO) "Derivatives" are parents, spouses, and unmarried children under 21 years of age. Other family members, such as siblings, married children, nieces, nephews, grandchildren, uncles, aunts, sisters-in-law, brothers-in-law, mothers-in-law, and fathers-in-law will not be considered by ICE for parole. The requirements for dependents to seek legal status in the United States are under the S visa program.

#### 9.3.1.2.4. (U) Employment Authorization

(U//FOUO) An alien granted SPBP or deferred action is eligible to receive an employment authorization document allowing him or her to work legally in the United States. Dependents and family members are also eligible for employment authorization. The indication of a need for employment authorization should be included in the initial SPBP or deferred action request and in any subsequent extension. Upon approval of the parole or deferred action, the control agent must submit an I-765, "Application for Employment Authorization," to his or her local CIS office with the SPBP or deferred action letter and the corresponding fee, which must be paid by the CHS. Agents should contact [redacted] for assistance with this process, if needed.

#### 9.3.1.2.5. (U//FOUO) Confidential Human Source Coordinator

(U//FOUO) The CA should coordinate with the CHSC in his or her FO when submitting an application for SPBP or deferred action. In addition, the CHSC should be made aware of all renewals, extensions, terminations, arrests and any other significant changes in the status of the alien. The CHSC functions as an important POC between the FO and [redacted]

### 9.3.1.3. (U//FOUO) Special Public Benefit Parole Process

#### 9.3.1.3.1. (U//FOUO) Request

(U//FOUO) To request an SPBP, the CA must contact the SPBP program manager at [redacted] for assistance with completing the SPBP application and to ensure field-wide compliance with ICE protocol and FBI policy. If the request does not meet the criteria, [redacted] will return the request to the requesting agent and provide the appropriate guidance. Once the template is complete, the request will be forwarded to LEPU at ICE for approval. It typically takes four to eight weeks for [redacted] to receive a decision from ICE. If an emergency parole is needed (i.e., for entry to the United States within 72 hours), the CA should contact its local Customs and Border Patrol (CBP) POC to facilitate the alien's entry (if possible). The SPBP request must also be submitted in order to receive approval for the alien to remain in the United States after entry is granted by CBP.

#### 9.3.1.3.2. (U//FOUO) Approval

(U//FOUO) When ICE receives an initial parole request, it sends a Notice of Request (NOR) to the Drug Enforcement Administration (DEA), the USMS, HSI, and the FBI. The NOR advises each agency that a parole has been requested for the individual and requests each agency to conduct database checks and concur or object to the parole. Once ICE has received the results, it makes a determination on the parole request and notifies [redacted] must notify the requesting agent of ICE's decision.

(U//FOUO) After ICE approves an SPBP, a Mandatory Tracking Requirement (MTR) form—which contains the details of the parole—is sent to [redacted]. The form indicates the length of the term for which the parole is granted (typically, one year) and the approval of any other requests, such as employment authorization, multiple-entry parole, and silent paroles.

(U//FOUO) After receiving the MTR form, [redacted] must provide the form to the control agent. The control agent should make several copies of the MTR form because it is used to report entry, departure, arrest, and any other status changes. The MTR also provides instructions regarding required reporting. All reporting should be sent directly to the [redacted] which will forward it to ICE. [redacted] functions as the sole POC for ICE (LEPU); therefore, agents should not contact ICE (LEPU) directly.

(U//FOUO) ICE will assign an International Affairs Office (IAO) number to the parolee. All future communications to FBIHQ regarding the parolee should reference the IAO case number, which can be found in the top right hand corner of the MTR form. This number is the means by which ICE tracks all parolees.

(U//FOUO) For parolees outside the United States, ICE will send an authorizing memorandum to the ICE attaché if there is an ICE presence in that country. If there is no ICE presence in the country where the parolee is located, ICE will ensure that a cable is sent to the issuing post specified in the SPBP template. The authorizing memorandum or cable authorizes the parolee to receive travel documents to enter the United States. ICE will also send an authorizing memorandum to CBP headquarters, and CBP will then notify the designated port of entry. The

authorizing memorandum notifies CBP of the name of the parolee, the designated port of entry, and the expected date of arrival.

#### 9.3.1.3.3. (U//FOUO) Extension

(U//FOUO) If, for operational purposes, the parolee must remain in the United States beyond the term of parole, a request for re-parole should be submitted to [redacted] using the SPBP application form. In the justification for the re-parole request, the agent must provide updated information summarizing the parolee's cooperation over the past year and information about anticipated activity (this does not apply to parole requests for dependants of parolees). Requests that are not updated will not be processed. The request should be submitted at least 30 days prior to the expiration date of the SPBP to allow time for ICE approval. ICE may limit the number of extensions granted.

#### 9.3.1.3.4. (U//FOUO) Agent Responsibilities

*(U//FOUO) Change of Date of Entry*

(U//FOUO) The CA should ensure that the parolee enters the United States within 30 days of the date on the MTR form. If entry into the United States will be delayed beyond 30 days, the CA must send an MTR form indicating the new proposed entry date to [redacted] must then provide the notification to ICE to keep the SPBP current. Absent this notification, ICE will terminate the parole, and no travel documents will be available to the parolee at the issuing post.

*(U//FOUO) Change of Issuing Post or Port of Entry*

(U//FOUO) If there is a need to change the issuing post or the port of entry after the approval of the parole, the CA must notify [redacted] by e-mail and include a justification for the change. In addition, the CA should contact the Legat in the country where the parolee will be traveling to secure the Legat's assistance.

*(U//FOUO) Travel Documents*

(U//FOUO) If the parolee will be arriving at a non-border port of entry, the CA should advise the parolee to obtain the documents authorizing travel to the United States from the issuing post. Usually, the issuing post is the U.S. Embassy, Consular Section, for the country from which the parolee is traveling. The parolee must bring four passport-sized photographs and identity documents to the interview at the issuing post. It is important to advise the parolee not to ask the Consular Section for a visa; he or she should request travel documents to the United States, pursuant to a parole. The travel documents consist of an I-512 form ("Authorization for Parole of an Alien into the United States") or a letter authorizing the parolee to board an aircraft bound for the United States. After the parolee receives the travel documents, he or she must travel to the United States within seven days, as the travel documents expire seven days after issue.

(U//FOUO) If arriving at a land border port of entry, the parolee does not receive travel documents from an issuing post. The parolee must present his or her identity documents to the CBP at the designated port of entry.

*(U//FOUO) Port of Entry*

(U//FOUO) At the port of entry, CBP officers will review the parolee's travel documents, conduct records checks, and issue and stamp the I-94 form ("Arrival/Departure Record"). The

CA should meet the parolee at the port of entry and ensure that the parolee arrives at the city and state where he or she will reside while in the United States.

*(U//FOUO) Report of Date of Entry*

(U//FOUO) After the parolee enters the United States, the CA must indicate the entry date on the MTR form and send the form to [redacted] will then notify ICE of the date on which the parolee entered the United States. The parole term will commence on the date the parolee entered the United States.

*(U//FOUO) Change of Control Agent (CA)*

(U//FOUO) The agent requesting the parole is, by default, the CA and is responsible for the parolee and all MTR reporting regarding the parolee. If the CA needs to transfer these responsibilities to another agent, he or she must send the MTR form to [redacted] requesting a change of control agent.

*(U//FOUO) Departure, Removal, and Absconding*

(U//FOUO) As noted earlier, it is the control agent's responsibility to exercise due diligence and ensure the departure or removal of the parolee after the parolee has finished his or her cooperation with the FBI. If the parolee departs voluntarily, the control agent must document the departure on the MTR form. If the parolee does not depart as required, the control agent should coordinate with the local ICE Enforcement and Removal Operations (ERO) FO to locate the parolee and take the individual into custody for removal proceedings. The control agent should note the name and contact information of the custodial ICE agent and the date of the parolee's custody on the MTR. In the event that the agent has exercised due diligence but cannot ensure the departure or removal of the parolee, the agent should send the MTR forms to [redacted] noting the efforts to locate the parolee and that the parolee has absconded. The control agent should coordinate with the local ICE FO to have an entry placed in ICE's TECS database. A copy of that entry must be sent, along with the MTR form, to [redacted] will in turn notify ICE of the change in status.

*(U//FOUO) Violation of the Law*

(U//FOUO) If a parolee is arrested or is known to have violated the law, the control agent must notify [redacted] by sending an MTR form with the arrest information or violation. The CA must also follow the procedure in Section 12, "Confidential Human Source Participation in Unauthorized Illegal Activity." If the FO supports continuing the parole, the control agent should request continuation of the parole in an LHM that documents the circumstances of the arrest and the current status of any prosecution and/or incarceration and provides justification for the continuation. [redacted] must notify ICE of the arrest and provide the supporting documentation and the request to continue the parole. If the CA does not request continuation of the parole, the parole will be terminated and the CA must coordinate with the local ICE office for the removal of the parolee.

### 9.3.1.4. (U) Silent Parole

(U//FOUO) A silent parole is requested when the control agent wants the alien to appear to be travelling on a visa, even though the alien is actually paroled into the United States. There are two types of silent paroles: "witting" and "unwitting." An example of a witting silent parole is when the CHS knows that he or she is being paroled in but the individual needs to appear for

operational security, to have entered on a visa. An example of an unwitting silent parole is when the agent wishes to have a pro forma (i.e., fake) visa issued to a subject who would otherwise be rejected for a visa or for entry and to have him or her paroled into the United States. Silent paroles must be coordinated with ICE, DOS, the FBI Legat, and CBP. An agent interested in silent parole should contact [redacted] for further guidance. ICE may limit the use of witting silent paroles.

### 9.3.2. (U) Deferred Action Program

(U//FOUO) As discussed earlier, an alien who is currently undergoing, or has ever undergone, ICE removal or deportation proceedings is not eligible for an SPBP. An alien who entered the United States with inspection, but is now without status, is also not eligible for an SPBP. Therefore, in order to utilize the alien as a CHS or a witness, the CA must request a deferred action from ICE for that person. The alternative is to have the alien voluntarily depart the United States and seek to reenter with an SPBP.

(U//FOUO) Under the deferred action program, an alien is not eligible for reentry after traveling outside the United States. The CA may, however, request an advance parole, which allows the alien to reenter the United States, if it is operationally necessary for the alien to travel outside the United States. The advance parole must be obtained prior to the alien departing the United States. Also, an alien may be granted work authorization when a deferred action has been approved by ICE. If the alien intends to work in the United States while under deferred action, the CA must request employment authorization approval in the initial application and in any requests for extension.

(U//FOUO) For more information on the advance parole, see subsection 9.3.3., "Advance Parole."

#### 9.3.2.1. (U) Authority

(U//FOUO) Deferred action is an administrative remedy of the last resort to delay an alien's removal from the United States. Deferred action does not confer any immigration status upon an alien or cure any defect in immigration status for any purpose. In addition, deferred action does not preclude ICE from commencing removal proceedings at any time against the alien. For these reasons, deferred action should not be requested if another type of administrative remedy, such as the SPBP or an extension of voluntary departure, is available. If deferred action is granted, however, ICE has the discretion to grant the alien work authorization. FOs should contact the [redacted] for guidance in seeking deferred actions.

#### 9.3.2.2. (U) Request

(U//FOUO) ICE policy and procedure for requesting deferred action depends on several factors, including the alien's custodial status and the ICE FO in which the alien resides. If the alien is in ICE custody, the agent should contact [redacted] for the procedure and documents for processing with ICE-ERO. If the alien is not currently in BOP or ICE custody, the deferred action must be requested from and approved by the SAC of the local DHS HSI FO. Because HSI FOs use different forms and procedures, the CA must contact [redacted] to determine the appropriate paperwork and procedure.

#### 9.3.2.3. (U) Approval

(U//FOUO) When ICE-ERO approves a deferred action, it sends a letter to [redacted] notifying [redacted] of the approval, term length, and conditions of the deferred action. The same letter is forwarded

to the ICE-ERO director in the jurisdiction where the alien is incarcerated. After receiving the deferred action letter, the local ICE-ERO office contacts the CA and coordinates the release of the alien into the custody of the requesting CA.

(U//FOUO) For aliens who are not in ICE custody, the notice of approval may come directly to the CA from the local HSI FO. In this case, the agent must provide a copy of the approval to [redacted]

#### 9.3.2.4. (U) Extension

(U//FOUO) If the alien is still being utilized at the end of the deferred action period, the CA must request an extension no later than 30 days before the expiration date. Similar to the initial request, the procedure for an extension varies between HSI FOs and ICE-ERO. The CA should coordinate with [redacted] for the appropriate forms and procedure.

#### 9.3.2.5. (U) Control Agent Responsibilities

*(U//FOUO) Reporting*

(U//FOUO) There is no MTR form for reporting status changes of aliens on deferred action. However, the CA is still required to immediately notify [redacted] if:

- (U//FOUO) The alien violates the law. If the FO wishes to continue the deferred action, the CA should make the request in an LHM that documents the circumstances of the arrest and the current status of any prosecution/incarceration and provides justification for continuing the deferred action. [redacted] must notify the HSI FO of the arrest and provide the supporting documentation and the request to continue the deferred action.
- (U//FOUO) The alien's cooperation is no longer needed.
- (U//FOUO) The alien has otherwise ended his or her cooperation, absconded, or departed the country.
- (U//FOUO) The CA for the alien has changed.

*(U//FOUO) Departure, Removal, and Absconding*

(U//FOUO) When a deferred action is terminated or expires, it is the CA's responsibility to exercise due diligence and ensure the departure or removal of the alien. If the alien departs the United States voluntarily, the CA must notify [redacted] of the departure. If the alien does not depart as required, the CA should coordinate with the local ICE-ERO FO to locate and take the alien into custody for removal. The CA should note the name and contact information of the custodial ICE agent and the date of the alien's custody. In the event that the agent has exercised due diligence but cannot ensure the departure or removal of the alien, the agent should notify [redacted] noting the efforts to locate the alien and that the alien has absconded. [redacted] will in turn notify the DHS HSI FO of the change in status. To complete the required reporting in these circumstances, the CA must complete a deferred action termination memo, which the [redacted] will provide to the agent.

### 9.3.3. (U//FOUO) Advance Parole

(U//FOUO) The CA may request an advance parole for an alien under deferred action or an SPBP without multiple entries. Advance paroles permit aliens to leave the country and reenter one time. Advance paroles are only permitted for operational travel and not for personal travel

and are not granted to family members. The CA should contact [redacted] for guidance on requesting an advance parole.

(U//FOUO) If the CA seeks to obtain legal status for the CHS following the CHS's assistance to the government, the SA may do so in certain circumstances (see subsection 9.3.4., below, and subsection 9.3.5., "Public Law 110 Program").

### 9.3.4. (U) S Visa Program

#### 9.3.4.1. (U) Nature and Purpose of the Program

(U//FOUO) The Violent Crime Control Act of 1994 created an "S" nonimmigrant classification under U.S. immigration law, known as an "S visa". An S visa may be made available to a very limited number of foreign nationals who have critical, reliable information that is necessary for the successful investigation or prosecution of a criminal organization or information concerning a terrorist organization. The S visa program does not result in an actual visa containing an "S" stamp. Nonimmigrant status enables an alien who is otherwise inadmissible to the United States to remain in the United States for a limited time. An S visa is not a mechanism to bring an alien into the United States and cannot be used to keep an alien in the United States for operational purposes. Other methods, such as the SPBP and/or deferred action, should be used for these purposes.

(U//FOUO) If approved for an S visa, an alien may be permitted to be lawfully present in the United States in a temporary, nonimmigrant status for up to three years. In practice, the S visa is not actually a visa; rather, it is intended for those already present in the United States. When approving an application for an S visa, the secretary of the DHS waives relevant grounds of inadmissibility that might otherwise prevent the person from becoming a lawful permanent resident. If the alien complies with the terms of admission, he or she may become eligible to apply for legal permanent resident (LPR) status, and possibly citizenship. The CA must consider this in determining whether to apply for a particular candidate. Prior to submitting an S visa application, the CA must also consider that several years may elapse from the time an S visa is granted until the adjustment to LPR status is completed.

(U//FOUO) There are two types of S visas for which a CHS may be sponsored. One is an S-5 nonimmigrant classification. The S-5 visa may be requested for an alien who possesses and is willing to provide critical, reliable information on a criminal organization to the requesting LE agency and who otherwise qualifies under Section 101(a)(15)(S) of the Immigration and Nationality Act and 8 Code of Federal Regulations § 214.2(t). The appropriate [redacted] unit must forward applications to the DOJ for initial approval; however, the DHS maintains final approval authority. Under amendments to the Violent Crime Control Act of 1994, a maximum of 200 aliens per FY may be granted S-5 visas.

(U//FOUO) The other type of S visa is an S-6 nonimmigrant classification. The S-6 visa may be requested for an alien who possesses and is willing to provide information on a terrorist organization, who will be placed in danger as a result of their cooperation; who is eligible for a monetary award under Section 36(a) of the State Department Basic Authorities Act of 1956, 22 U.S.C. § 2708(a); and who otherwise qualifies under Section 101(a)(15)(S) of the act and under 8 Code of Federal Regulations § 214.2(t). The CA must provide a nomination letter to the [redacted] on behalf of the CHS, stating the accomplishment(s) the CHS has made on behalf of the FBI (e.g., assisted in preventing a terrorist act from taking place). For S-6 non-immigrant visas, the

DOJ exercises joint responsibility to adjudicate requests by LE agencies. A maximum of 50 S-6 visas are available to aliens each year.

#### 9.3.4.1.1. (U) S Visa Program and CHS Involvement in Possible UIA

(U//FOUO) Once the S visa has been issued, if the CA reasonably believes the CHS has engaged in UIA, the CA must notify the [redacted] and the [redacted] must notify ICE to determine what action must be taken. See also Section 12, "Confidential Human Source Participation in Unauthorized Illegal Activity."

#### 9.3.4.2. (U) S Visa Application Process

(U//FOUO) An S visa request must be documented on a DOJ supplemental worksheet (available on the [redacted]) and approved by an SAC. The worksheet must then be forwarded to the appropriate [redacted], which must coordinate the application process with the DOS and OEO, DOJ. In addition to the administrative data required on the worksheet, the request must include:

1. (U//FOUO) The significance of the investigation.
2. (U//FOUO) The significance of the CHS's cooperation.
3. (U//FOUO) The basis of the request for S visa status. This section should set forth, in a quantitative fashion, the accomplishments based on the CHS's cooperation (e.g., number of arrests, indictments, convictions, seizures, disruptions, dismantlement, and the like). Furthermore, if submitting an S-5 request (criminal), the prosecutorial phase of the investigation should be completed before submitting an S visa application.
4. (U//FOUO) The names of family members for whom S visas are sought (if applicable).
5. (U//FOUO) An evaluation of the threat to the alien.
6. (U//FOUO) Preexisting grounds of excludability (e.g., pending criminal charges).
7. (U//FOUO) An LHM from the FO SAC endorsing the request.
8. (U//FOUO) A separate and completed form I-854, "Inter-Agency Alien Witness and Informant Record," for the principal alien and each family member, if the alien is married or has children or parents. (Note that, although Part 3 of this form states that it should be filled out "if applicable," the U.S. Attorney's signature—not that of the AUSA—is mandatory for the application to be accepted by DOJ.)
9. (U//FOUO) A separate and completed form G-325A for the principal alien and each family member.
10. (U//FOUO) A separate, current (within 30 days) NCIC record check (i.e., "rap sheet") for the principal alien and each family member who is 16 years of age or older. In cases where a criminal record does not exist, the CA must submit a printout showing a negative inquiry.
11. (U//FOUO) Criminal Justice Information Services (CJIS) checks for both the principal alien and derivatives.
12. (U//FOUO) An S visa application that includes a pre-sentence report and/or plea agreement for all aliens who have been convicted of a federal crime within the last three to five years.

13. (U//FOUO) Four applicant fingerprint cards [redacted] containing a complete set of fingerprints and signatures for the principal alien and each family member who is 12 years and 9 months or older.

14. (U//FOUO) Two recent, color, frontal-view passport photos with white backgrounds for the principal alien and each family member, with names and alien numbers on the backs of the photos.

15. (U//FOUO) Copies of passports in their entirety (i.e., front and back covers and all pages, including blank pages) for the principal alien and his or her family members.

16. (U//FOUO) Copies of any documents establishing qualifying family relationships. If the spouse of the principal alien is listed on the application as a family member, a copy of the marriage certificate is required (if the principal alien was previously married, a copy of the divorce decree from the prior marriage should also be submitted). If a child of the principal alien is listed on the application as a family member, a copy of the child's birth certificate is required. A translation must accompany all documents and certificates, if applicable. If no documentation is available, contact the [redacted]

#### 9.3.4.2.1. (U) International Travel for S Visa CHSs

(U//FOUO) The USCIS makes the final decision as to whether to approve an S visa. If approved, the S visa does not authorize the alien to travel abroad. If circumstances require the individual to travel outside the United States for operational or exigent personal reasons (e.g., family death), the SA must submit a request to the appropriate [redacted] unit for advance parole or a comparable authorization to enable the individual to reenter the United States. Advance paroles are available in very limited circumstances to LE agencies for S visa applicants who travel internationally and need documentation to reenter the United States. For questions regarding advance parole criteria, initiating an S visa, or determining whether or not the CHS qualifies for an S visa, contact the appropriate [redacted] unit.

#### 9.3.4.2.2. (U) CHS S Visa Work Authorization

(U//FOUO) Upon the initial submission of the S visa application to the DOJ, the CA may request a work authorization from DHS through the appropriate [redacted] unit. The CHS must pay the costs associated with the S visa application. The FBI may not pay or reimburse the fees as a CHS expense. In addition, the FBI cannot pay or reimburse the CHS for personal living expenses during the approval process.

### 9.3.5. (U) Public Law 110 (PL-110) Program

(S//NF) The PL-110 Program, administered by the CIA, provides permanent resident alien status to certain alien CHSs who provide significant assistance in the interest of national security or to further a national intelligence mission. In the National Security Branch (NSB), CHSs who provide exceptional cooperation regarding counterterrorism, counterintelligence, and intelligence matters may be eligible for a PL-110. Only [redacted] PL-110s a year may be approved for all agencies.

(S//NF) A CA must send a request for CHS PL-110 status to the appropriate [redacted] unit, which then must coordinate with the DAD of the relevant operational unit, the DOJ, ICE, and the CIA. The CA must provide the following information to the FIMS in an LHM:

- (S//NF) The CHS's true name and the names of any immediate family members included in the request

- (S//NF) Biographical data
- (S//NF) Immigration status
- (S//NF) Relatives in the United States
- (S//NF) Financial status
- (S//NF) Employment
- (S//NF) Criminal history or criminal activity
- (S//NF) Whether the CHS's current and future financial status is stable or whether the government incurs a financial obligation in connection with the CHS's resettlement
- (S//NF) Details about the CHS's relationship with the FBI and the CIA, including the CHS's payment history and a comprehensive description of significant contributions the CHS has made in furtherance of national security

### 9.4. (U) Individuals Seeking Asylum

(S//NF) An individual seeking asylum may be opened as a CHS in accordance with this PG. The

[redacted]

### 9.5. (U//FOUO) Notional Documents

(U//FOUO) Notional documents, such as permanent resident alien cards (i.e., "green cards") or employment authorization cards, are effective tools for LE and intelligence operations and may be requested for the CHS. Notional documents are backstopped, but are for "flash" purposes only and do not convey any benefits. For international travel, the CHS still needs a passport or a reentry permit.

(U//FOUO) To obtain notional documents, the CA must submit to the appropriate [redacted] unit an LHM detailing a summary of the investigation; a justification for the requested immigration benefit and/or document; the CHS's role and access to critical information; the effect the CHS's participation will have on the case; and the CHS's identifying information (i.e., name, alien number, sex, date-of-birth, and country-of-birth). All TECS, NCIC, and CIS system checks must be completed and the results attached. Additional forms, such as the as I-89 cards, I-765 ("Application for Employment Authorization") forms, and passport photos may be required for the request. (See the [redacted] for information regarding these forms.)

(U//FOUO) After completion and review, the [redacted] coordinates with and forwards the appropriate documentation to DHS for approval.

(U//FOUO) Any notional document approved for use by the CHS must be available to the CHS only during operational events. The document must be retrieved and maintained in a locked storage container within the FBI office space by the CA after each operational use.

# 10. (U//FOUO) Operation of Confidential Human Sources

## 10.1. (U//FOUO) CHSs Who May Testify in a Court or Other Proceeding

(U//FOUO) The CA or co-CA must document to the CHS file any FPO approvals, notifications, or coordination required in this PG for CHS operational activities (e.g., payments, Tier I and Tier II OIA) that may become an issue in court if it is necessary for the CHS to testify.

(U//FOUO) Whenever it becomes apparent that a CHS may have to testify in a court or other proceeding in which he or she is providing assistance to the FBI, the SA must advise the CHS and document the advisement in the source contact report (FD-1023).

(U//FOUO) The CA or co-CA should be aware that the manner in which a CHS is tasked may subject the CHS to having to testify, even if the CHS's testimony is not anticipated or desired. For instance, if the CHS is tasked to gather physical or documentary evidence, make consensual recordings, or engage in OIA, the CHS may later be required to testify. Accordingly, the CA or co-CA must inform the CHS of this prior to tasking the individual in this manner.

(U//FOUO) Unanticipated situations may also arise that require a CHS to testify, even though the CHS has not previously agreed to do so. For example, if a CHS becomes aware of exculpatory information or becomes the single source of information for use in a trial, it may be necessary for the CHS to testify. If there is a possibility that a court will require the disclosure of a CHS's identity and the FO objects to this disclosure, the CA or co-CA may discuss with the FPO whether the case should be dismissed. (See Section 15, "Disclosure of a Confidential Human Source's Identity.")

## 10.2. (U) Electronic Communications With a CHS

(U//FOUO) E-mail, text message, facsimile, and other electronic communications between an SA and a CHS are discouraged because these methods are easily intercepted [redacted] and can compromise the CHS. Depending upon the circumstances, in order to protect the CHS and the operation, consideration must be given to the type of investigation the CHS is supporting, the specific interactions required with the CHS, the technical proficiency of the CHS, and whether technical equipment needs to be supplied to the CHS. Overt FBI purchase of equipment supplied to the CHS and the use of overt FBI equipment to communicate with the CHS are not recommended, except in very limited circumstances. Issues related to communications are complex and possible solutions to hurdles encountered can be discussed with the program manager for the [redacted] program. The use of solutions proposed by [redacted] must be documented in the CHS file.

(U//FOUO) In addition, the above-listed electronic communication tools or devices diminish the SA's ability to observe the CHS. Consequently, the SA must exercise caution in using them; in-person contact is the preferred method of interaction with the CHS. If any of the above methods are used, their use must be documented in the CHS file. In addition, agents should be aware that all communications with a testifying CHS will likely be produced in discovery. Therefore, agents must ensure that all communications are essential to operations and professional in content.

(U//FOUO) SSA approval is required for all interaction with a CHS via Internet-based or electronic communication, including, but not limited to, e-mail, text, facsimile, social networks, forums, cloud computing, and app-based connections. This approval must be properly

documented in the CHS file. These communication methods should only be used when operationally necessary, and proper consideration should be given to operational security, including the use of misattributed Internet connections, encryption, and other means. Additional guidance on proper operational security can be provided by [redacted]

(U//FOUO) Use of the above electronic communication methods—as well as telephonic contact—with a CHS who is operated in a foreign country is addressed in Section 19, "Extraterritorial Operations."

(U//FOUO) Additional guidance on secure communications with a CHS can be provided by the FBIHQ operational divisions and the program manager for [redacted] program.

### 10.3. (U) Consensual Recording

(U//FOUO) Consensual monitoring by a CHS must comply with the AGG-Dom and DIOG subsection 18.6.1.

### 10.4. (U) Undercover Operation

(U//FOUO) If it is necessary for a CHS to be involved in a UCO, the CHS's participation requires the approval of the FO and, if it is a Group I UCO, of FBIHQ (see DIOG subsection 18.6.13). Upon approval of the UCO, however, the FO still must separately approve the specific activities for the CHS within the UCO (e.g., OIA, interdivision travel, undisclosed participation) in accordance with this PG. The OIA must be documented through Delta. In addition, although the UCO proposal may contain an estimated amount of funding required for CHS services and/or expenses associated with the UCO, these CHS payments are not approved through the UCO or covered by UCO funding. All payment requests for CHS services and expenses in the UCO must be justified and processed in accordance with Section 17, "Confidential Human Source Financial Matters."

### 10.5. (U//FOUO) Undisclosed Participation

(U//FOUO) Undisclosed participation by CHSs must comply with the AGG-Dom and DIOG Section 16.

### 10.6. (U//FOUO) Alias/False Identification

(U//FOUO) The FBI's issuance of an AFID to CHSs is only allowed in extraordinary circumstances. One of the few areas where AFIDs for CHSs have been granted is in Medicare fraud investigations, where former FBI employees meeting relevant age requirements are opened as CHSs (see subsection 7.15., "Former FBI Employees and Persons With a Present or Former Relationship With an FBI Employee"). AFID may not be issued to a CHS for the purpose of providing security following his or her cooperation. The CA or co-CA must use other methods to provide protection, such as a lump-sum payment to relocate the CHS (see subsection 17.14., "Lump-Sum Payments," and subsection 17.6.6., "Relocation"), a safe house, or the WSP (see Section 8, "Witness Security Program").

(U//FOUO) A request for an AFID for a CHS must contain compelling justification—including a description of the proposed operation of the CHS—and specify whether the CHS will operate using the AFID on a full-time or part-time basis. In the FO, the request must be approved by the undercover coordinator (UCC) and the SAC. The request must then be sent to the [redacted] which will coordinate the approval of the request by the operational unit, FBIHQ UC program manager, the [redacted] and the [redacted]

The [redacted] advises the FO of the final decision. Documentation related to the request and outcome must be placed into the CHS file.

(U//FOUO) If a CHS is issued an AFID, the FO is responsible for ensuring that it is used in compliance with the [redacted] Under all circumstances, however, the AFID must only be made available to the CHS during operational events and retrieved by the FBI after each operational use. The AFID must be maintained in an FO safe or authorized security container when not in use.

### 10.7. (U) Obtaining Information About a Subject's Pending Charges or Legal Defense Plans

(U//FOUO) If a CHS is in a position to obtain information from a defendant who is facing pending criminal charges for which the defendant's Sixth Amendment right to counsel has attached, the CHS must be instructed not to solicit information from the defendant regarding the pending charges. A subject's Sixth Amendment right attaches when a prosecution is commenced (i.e., at or after the initiation of adversarial judicial criminal proceedings—whether by way of a formal charge, a preliminary hearing, an indictment, a criminal information document, or an arraignment).

(U//FOUO) Nevertheless, a CHS may be directed to 1) become a passive listener to report, but not solicit, statements by a defendant about pending charges or 2) obtain information from a defendant about a matter that is separate from the one(s) pending against the defendant.

(U//FOUO) In certain circumstances, a CHS's contact with a defendant who is represented by counsel, but against whom charges are not pending, may be limited by other laws (see the Citizen's Protection Act, codified at 28 U.S.C. § 530B). On any occasion when a CHS is directed to have contact with a person who is represented by an attorney, it is recommended that the CA consult with the FO's CDC.

(U//FOUO) Finally, the CA must instruct the CHS not to interfere with the defendant's attorney-client relationship. For example, the CHS should not make disparaging remarks about the attorney or about the way in which the defendant should cooperate with the attorney.

(U//FOUO) Any questions about the content of this subsection should be directed to the assigned AUSA or to the FO CDC.

### 10.8. (U//FOUO) Use of a CHS Associated With a Wire or Electronics Service Provider

(U//FOUO) Before operating a CHS who is employed by a wire or electronic communications service provider or who owns or operates a company providing such a service (i.e., a CHS associated with a telephone company or an internet service provider), the CA or co-CA must consult the CDC to ensure that the use of the CHS's does not infringe upon the First Amendment right to free speech.

(U//FOUO) The Electronic Communications Privacy Act (ECPA) establishes limitations on the government's access to records and content held by wire or electronic communications service providers, including telephone companies and companies offering communication facilities through the Internet. Thus, those restrictions limit the FBI's ability to obtain records from a CHS who is employed by a wire or electronic communications service provider or who owns or operates a company providing such a service. Furthermore, the Fourth Amendment protects

service providers' customers from the disclosure of the contents of their communications to the government.

(U//FOUO) Therefore, as a general rule, the FBI may not accept records or the content of communications from a CHS employed by a wire or electronic communications service provider or who owns or operates such a company. The use of a CHS to voluntarily provide information to the FBI does not constitute compliance with ECPA or the Fourth Amendment. The CA or co-CA may only obtain such information through applicable legal processes (e.g., a grand jury subpoena, a National Security Letter [NSL], a search warrant, or an ELSUR order).

(U//FOUO) The CDC should be consulted if there are any questions about what information may be obtained from such a CHS in compliance with ECPA.

### 10.9. (U) Elected or Appointed Government Officials

(U//FOUO) The FBI may accept information concerning alleged violations of law or other matters within FBI jurisdiction from government officials. The FBI may not recruit or operate CHSs for the sole purpose of collecting information concerning the political beliefs or personal lives of individuals within a governmental body or the private or confidential deliberations of that body. Furthermore, the FBI may not knowingly influence or attempt to influence any action of a USG body, unless it is done in furtherance of a compelling governmental interest. If the investigation plans any activity that may influence a USG body, the SSA, CA, or co-CA must consult the CDC. Additionally, this type of activity may trigger review and approval requirements for undisclosed participation and must comply with the AGG-Dom and DIOG Section 16.

### 10.10. (U//FOUO) Employees of Financial Institutions

(U//FOUO) If a CHS is an employee of a financial institution, the CA may not task the CHS to provide or knowingly accept information that violates the provisions of the Right to Financial Privacy Act of 1978 (12 U.S.C. § 3402). The act prohibits the FBI from obtaining the financial records of any customer from a financial institution outside of specified formal processes, such as subpoenas and search warrants.

### 10.11. (U//FOUO) Employees of Educational Institutions

(U//FOUO) The Family Educational Rights and Privacy Act (the Buckley Amendment) establishes limitations on the government's access to student educational records held by institutions of higher learning. These restrictions limit the FBI's ability to obtain records from a CHS who is employed by an educational institution in any capacity (e.g., as a faculty member, a librarian, and the like). Therefore, as a general rule, the FBI may not accept records from a CHS employed by an educational institution.

(U//FOUO) One major exception to this rule is that a CHS may provide "directory information," since this information is not protected and may be voluntarily produced under certain circumstances. Furthermore, records of campus police are also subject to voluntary production. The CDC should be consulted if there are any questions about what information may be obtained from such a CHS in compliance with the Buckley Amendment.

### 10.12. (U//FOUO) Use of a Sub-Source

(U//FOUO) A sub-source is any individual who directly acquires information that is then provided to the FBI by an FBI CHS as a result of the CHS being tasked. Examples of persons not considered sub-sources, by definition, are as follows:

- (U//FOUO) Contacts with whom the CHS has familial communications and whose information he or she then shares with the FBI
- (U//FOUO) Contacts with whom the CHS has business-related communications and whose information he or she then shares with the FBI
- (U//FOUO) Acquaintances or nonpersistent contacts with whom the CHS has communications and whose information he or she then shares with the FBI

(U//FOUO) In domestic operations, the CA or co-CA must not task, direct, or control a sub-source through the CHS. Any direct or indirect instruction through a CHS to engage in information-collection activity is considered tasking and is prohibited in domestic operations.

(U//FOUO) For information regarding the use of a sub-source in extraterritorial (ET) operations, see Section 19, "Extraterritorial Operations."

### 10.13. (U//FOUO) Use of CHS Information in a Foreign Intelligence Surveillance Act Affidavit

(U//FOUO) If an FO has CHS information that supports probable cause necessary for a Foreign Intelligence Surveillance Act (FISA) application, that information may be used without revealing the identity of the CHS. Upon SSA approval, the CA or co-CA must provide the FBIHQ operational unit with the CHS's file number, the length of time the individual has been a CHS, and a statement regarding the CHS's reliability and whether the information has been corroborated. All information provided to support the FISA application, including the CHS's information, must be documented in the CHS file. The CA or co-CA should also be prepared to provide the following information, upon request, to the operational unit for distribution to the DOJ's NSD or for use in the FISA application:

- (U//FOUO) Whether or not the CHS was paid (SAs may use general terms so that no exact amounts are given—for example, "the CHS was paid a modest fee for information.")
- (U//FOUO) All convictions against the CHS
- (U//FOUO) Any other Brady Act/impeachment information

### 10.14. (U//FOUO) CHS Prioritization System

(U//FOUO) The CPS is a tool in Delta that was established to determine CHS prioritization based on the risk of operation. The tool is incorporated into the Sensitive Information tab in Delta, and the information entered about the CHS must be updated on a quarterly basis. See Section 20, "Confidential Human Source Validation," for more information.

# 11. (U) Department of Justice Notification Requirements

(U//FOUO) This section describes situations involving a CHS that require the FBI to notify certain components of the DOJ, in accordance with the AGG-CHS. The DAG must approve exceptions to these notification requirements, as set forth in subsection 11.8., "Exceptions to the DOJ Notification Requirements." All notifications discussed in subsections 11.3. through 11.5. must be made in writing and approved by the SSA.

## 11.1. (U) Notification Designees

(U//FOUO) An SAC and a CFP may designate (if both concur) particular individuals in their respective offices to carry out the functions assigned to them in subsections 11.2. ("Notification to DOJ of Unauthorized Illegal Activity") through 11.7. ("Responding to Requests from FPO Attorneys Regarding a CHS") and subsection 11.9., "DOJ Review of FBI CHS Files for Non-Testimonial CHSs."

## 11.2. (U) Notification to DOJ of Unauthorized Illegal Activity

(U//FOUO) For notification procedures related to CHS UIA, see Section 12, "Confidential Human Source Participation in Unauthorized Illegal Activity."

## 11.3. (U) Notification to DOJ of the Investigation or Prosecution of a CHS

(U//FOUO) If an SA has reasonable grounds to believe that the alleged felonious activity of a current or former CHS is, or is expected to become, the basis of a prosecution or investigation by an FPO, the SA must immediately notify a DOJ CHSC or the assigned FPO attorney of that individual's status as a current or former CHS. With respect to a former CHS whose alleged felonious activity is, or is expected to become, the basis of a prosecution or investigation by a state or local prosecutor's office, the DOJ CHSC or assigned FPO attorney must be immediately notified, but only if the SA has reasonable grounds to believe that the CHS's prior relationship with the FBI is material to the prosecution or investigation.

(U//FOUO) Whenever such a notification occurs, the DOJ's CHSC or the assigned FPO attorney is responsible for notifying the CFP. The CFP and FBI SAC (or designees), with each other's concurrence, must notify any other federal, state, or local prosecutor's office, or LE agency that is participating in the investigation or prosecution of the CHS. The notification to other prosecutors or LE agencies must be documented in the CHS file.

(U//FOUO) The SA's notification to the DOJ CHSC or FPO attorney must be made in writing, approved by the SSA, and maintained in the CHS's validation sub-file.

## 11.4. (U) Notification to DOJ Regarding Certain Federal Judicial Proceedings

(U//FOUO) An SA must immediately notify the appropriate DOJ CHSC or the assigned FPO attorney whenever the agent has reasonable grounds to believe that:

- (U//FOUO) A current or former CHS has been called to testify by the prosecution in any federal grand jury or judicial proceeding.
- (U//FOUO) The statements of a current or former CHS have been, or will be, utilized by the prosecution in any federal judicial proceeding.

- **(U//FOUO) An FPO attorney intends to represent to a court or jury that a current or former CHS is or was a coconspirator or other criminally culpable participant in any criminal activity.**

**(U//FOUO) The notification must be made in writing, approved by the SSA, and maintained in the CHS's validation sub-file.**

### 11.5. (U) Notification to DOJ of Privileged or Exculpatory Information

(U//FOUO) If an FPO is participating in the conduct of an FBI investigation that is utilizing a CHS or working with a CHS in connection with a prosecution, the CA or co-CA must notify the FPO attorney assigned to the matter—in advance, whenever possible—if the CA or co-CA has reasonable grounds to believe that the CHS will obtain or provide information that is subject to, or arguably subject to, a legal privilege of confidentiality belonging to someone other than the CHS. Documentation that the notification has been made by the CA or co-CA must be placed in the CHS Delta file.

(U//FOUO) Whenever an SA knows or reasonably believes that a current or former CHS has information that is exculpatory as to a target of or a defendant (including a convicted defendant) in a federal, state, or local investigation or case, the FBI agent must disclose the exculpatory information to either the assigned FPO attorney that is participating, or had participated, in the conduct of that investigation or to the DOJ CHSC. The disclosure notification must be made in writing, approved by the SSA, and maintained in the CHS's validation sub-file.

(U//FOUO) In turn, the assigned FPO attorney or the DOJ CHSC is responsible for disclosing the exculpatory information to all affected federal, state, and local authorities. In the event that the disclosure would jeopardize the security of the CHS or seriously compromise an investigation, the FPO attorney or DOJ CHSC must refer the matter to the HSRC for consideration, except for matters related to an international terrorism or national security investigation. The latter must be referred to the AAG of the NSD (or designee). The basis for referring the matter to the HSRC or the AAG of NSD (or designee) must be documented in the referral and placed into the CHS file.

### 11.6. (U//FOUO) Notification to DOJ Upon Naming a CHS as an Interceptee or a Violator in an Electronic Surveillance Application

(U//FOUO) An SA must not name a CHS as an interceptee or a violator in an affidavit in support of an application for an ELSUR order made pursuant to 18 U.S.C. § 2516, unless the SA believes that:

- (U//FOUO) Omitting the name of the CHS from the affidavit would endanger the CHS's life or otherwise jeopardize an ongoing investigation.
- (U//FOUO) The CHS is a bona fide subject of the investigation based on the CHS's suspected involvement in UIA. See subsection 11.2., "Notification to DOJ of Unauthorized Illegal Activity."

(U//FOUO) If the CHS is named in an ELSUR affidavit, the SA must inform the FPO attorney making the application and the court to which the application is made of the CHS's actual status. The SA notification to the FPO attorney must be made in writing, approved by the SSA, and documented in the CHS's main sub-file.

### 11.7. (U//FOUO) Responding to Requests From FPO Attorneys Regarding a CHS

(U//FOUO) For criminal matters arising under or related to the AGG-CHS, upon request by an appropriate FPO attorney, the CA or co-CA, in coordination with the CHSC, must promptly provide to the FPO attorney all relevant information concerning a CHS, including whether the individual is a current or former CHS for the FBI. The dissemination of the relevant information to the FPO must be approved by the SSA and documented to the CHS file.

(U//FOUO) If the SAC has an objection to providing this information based on the specific circumstances of the case, he or she must explain the objection to the FPO attorney making the request, and any remaining disagreement as to whether the information should be provided to the FPO attorney must be resolved pursuant to subsection 1.5.1., "AGG-CHS and AGG-Dom Exceptions and Dispute Resolution."

### 11.8. (U) Exceptions to the DOJ Notification Requirements

(U//FOUO) The Director of the FBI, with the written concurrence of the DAG, may withhold any notification required pursuant to subsection 11.2., "Notification to DOJ of Unauthorized Illegal Activity," through subsection 11.7., above, if the SAC and DAG determine that the identity, position, or information provided by the CHS warrants extraordinary protection for sensitive national security reasons. Any SAC determination to withhold notification, along with the concurrence of the DAG, must be documented by the CA or co-CA and maintained in the CHS's main file.

### 11.9. (U//FOUO) DOJ Review of CHS Files for Non-Testimonial CHSs

(U//FOUO) If an FPO attorney seeks to review the file of a CHS who is not expected to testify, the CA or co-CA must advise the FPO attorney to submit a written request to the FO CDC. The FPO attorney's request must specify the information sought and provide justification for the review. After consulting with the CDC and ASAC, the SAC must issue a written response to the FPO attorney outlining the parameters of any permitted review. The SAC response and the FPO attorney request must be documented to the CHS file.

(U//FOUO) If the SAC and FPO agree on the terms of the review, the CHSC must make arrangements for the CHS file review in FBI office space. The FPO attorney is not permitted to remove copies of CHS file material from FBI space without CDC approval. The CA or co-CA should document this agreement in the administrative portion of the CHS file.

(U//FOUO) The CA or co-CA must prepare a record of the FPO attorney's CHS file review, which must include the FPO attorney's request and the SAC's response, the date of the CHS file review; the identity of the FPO reviewer; the method of review; the identification of any documents reviewed and (if applicable) of any copies of CHS file material removed from the FBI office by the FPO reviewer; and the written approval of the CDC permitting the document removal.

(U//FOUO) The resolution of any disagreement between the FPO attorney and the CDC regarding the printing and release of documents from the CHS file must be done in accordance with subsection 1.5.1., "AGG-CHS and AGG-Dom Exceptions and Dispute Resolution."

(U//FOUO) See also the DAG memorandum titled, "Guidance on the Federal Bureau of Investigation's (FBI) Administration of Confidential Human Sources and Its Impact on the Discovery Obligations of Prosecutors" (January 15, 2009).

# 12. (U) Confidential Human Source Participation in Unauthorized Illegal Activity

## 12.1. (U) Notification Process

(U//FOUO) According to the AGG-CHS, if an FBI agent has reasonable grounds to believe that a CHS has engaged in UIA (other than minor traffic offenses), the CHS must be closed, unless SAC approval for continued use is obtained (see subsection 12.2., below). The SA must promptly notify DOJ's CHSC or the assigned FPO attorney of the UIA and the reasonable grounds upon which the FBI believes it has occurred. Reasonable grounds exist, for example, when an SA has knowledge of a pending state or federal investigation of the CHS; pending criminal charges against the CHS; or an admission from the CHS, or if the SA has information from two or more independent sources, or from one credible source, that the CHS has engaged in illegal activity. The SA must make the notification even if the CHS will be closed as a result of the illegal activity. The notification to DOJ must be made in writing, approved by the SSA, and documented in the CHS main file.

(U//FOUO) If the CHS's continued use is desired, approval must be obtained in accordance with subsection 12.2.

(U//FOUO) After being notified by the FBI, the DOJ's CHSC or assigned FPO attorney is responsible for notifying the following FPOs of the CHS's criminal activity and the individual's status as a CHS:

- (U//FOUO) The FPO in whose district the criminal activity primarily occurred, unless a state or local prosecuting office in that district has filed charges against the CHS for the criminal activity and there is no basis for federal prosecution in that district
- (U//FOUO) The FPO attorney, if any, who is participating in the conduct of an investigation that is utilizing the CHS or is working with the CHS in connection with a prosecution
- (U//FOUO) The FPO attorney, if any, who authorized the CHS to engage in OIA

(U//FOUO) Whenever these notifications are provided, the CFP and the SAC (or the individual to whom authority has been delegated in accordance with subsection 11.1., "Notification Designees"), with the each other's concurrence, must notify any state or local prosecutor's office which has jurisdiction over the CHS's criminal activity and which has not already filed charges against the CHS for the criminal activity, that the CHS has engaged in criminal activity. If the state and local prosecutor's office is known to already be aware of the CHS's criminal activity, then notification by the CFP and SAC is unnecessary. The CFP(s) and the SAC(s) are not required to, but may (with each other's concurrence) also notify the state and local prosecutor's office of the person's status as a CHS. These notifications must be documented in the CHS's main file.

## 12.2. (U//FOUO) Request for Approval of the Continued Operation of a CHS

(U//FOUO) When a CA has reasonable grounds to believe that a CHS has engaged in UIA, but wishes to continue to use the CHS, in addition to reporting the UIA to DOJ in accordance with subsection 12.1., "Notification Process," the CA must submit a request for continued operation to the SAC (non-delegable) for approval (see subsection 18.1.2., "Closing a CHS for Cause").

(U//FOUO) The request must address:

- (U//FOUO) The seriousness and duration of the illegal activity.
- (U//FOUO) Whether the CHS has previously engaged in UIA (and, if so, the details of that activity).
- (U//FOUO) Whether the CHS has ignored any previous admonishments.
- (U//FOUO) The importance of the CHS to the FBI's mission.
- (U//FOUO) The risk to the public from the CHS's illegal activity.
- (U//FOUO) The likelihood that the CHS will engage in UIA in the future.

(U//FOUO) If the SAC approves the continued use of the CHS, the CA must re-admonish the CHS with regard to participation in UIA and remind the CHS that the individual has no immunity from prosecution for the unauthorized activity. The CA must document the request to continue CHS use and the outcome of the request in the CHS file.

### 12.3. (U//FOUO) UIA Resulting From Violation of the Authorization for Illegal Activity

(U//FOUO) When an CA has reason to believe that a CHS has violated the terms of his or her authorization for participating in OIA, the SA must immediately revoke the CHS's authorization and follow the procedures outlined in subsection 13.8., "Revocation of OIA Authorization."

# 13. (U//FOUO) Confidential Human Source Participation in Otherwise Illegal Activity

(U//FOUO) Under certain circumstances described in this section, a CHS may be authorized to participate in certain illegal activity referred to as "otherwise illegal activity." OIA is defined as any activity that would constitute a criminal violation under federal, state, or local law if a person were to engage in it without authorization. The OIA must be reasonable under the circumstances, which include the scope, geographic area, and duration of the unlawful activity.

## 13.1. (U) Prohibited Activities

(U//FOUO) According to the AGG-CHS, the FBI must never authorize a CHS to:

- (U//FOUO) Participate in any act of violence, except that the CHS may take reasonable measures of self-defense in an emergency to protect his or her own life or the lives of others against wrongful force.
- (U//FOUO) Participate in an act designed to obtain information for the FBI that would be unlawful if conducted by an LE agent (e.g., breaking and entering, illegal wiretapping, illegal opening or tampering with mail, or trespass amounting to an illegal search).

(U//FOUO) In addition, CAs, co-CAs, and SSAs must ensure that any dangerous commodity or item (such as a firearm, body armor, explosives, and the like) does not leave law enforcement (LE) control[2] and that drugs do not leave LE control absent specific approval from the appropriate headquarters official.

## 13.2. (U) Tier I OIA

### 13.2.1. (U) Tier I OIA Definition[3]

(U//FOUO) The AGG-CHS defines Tier I OIA as any activity that would constitute a misdemeanor or felony under federal, state, or local law if engaged in by a person acting without authorization and which involves any of the following activity:

- (U//FOUO) The commission or the significant risk of the commission, of any act of violence by a person or persons other than the CHS.[4]
- (U//FOUO) The corrupt conduct, or the significant risk of corrupt conduct, by an elected public official, a public official in a high-level decision-making or sensitive position in federal, state, or local government.

---

[2] (U) Per AGG-Dom and AGG-UCO, in a controlled transaction, the item(s) will be monitored by the FBI and returned or seized at the conclusion of the transaction.

[3] (U//FOUO) While the AGG-CHS definition of Tier 1 violations generally does not include potential violations of the material support statutes, inasmuch as the below-listed six factors are rarely involved, FBI practice is to treat potential material support statute violations as Tier 1 violations, requiring the approval of the AD, Counterterrorism Division (CTD) and of the DOJ.

[4] (U) Bookmaking that is significantly associated with, or substantially controlled by, organized crime ordinarily will be within the scope of this definition. Thus, for example, where bookmakers have a financial relationship with members or associates of organized crime, and/or use members or associates of organized crime to collect their debts, the conduct of those bookmakers would create a significant risk of violence, and would therefore fall within the definition of Tier I OIA.

- (U//FOUO) The manufacturing, importing, exporting, possession, or trafficking of controlled substances in a quantity equal to or exceeding those quantities specified in United States Sentencing Guidelines (USSG) 2D1.1(c)(1).
- (U//FOUO) The financial loss, or the significant risk of financial loss, in an amount equal to or exceeding those amounts specified in USSG 2B1.1 (b)(1)(I).[5]
- (U//FOUO) A CHS providing to any person (other than an FBI agent) any item, service, or expertise that is necessary for the commission of a federal, state, or local offense that the person would otherwise have difficulty obtaining.
- (U//FOUO) A CHS providing to any person (other than an FBI agent) any quantity of a controlled substance, an explosive, firearm, other dangerous weapon, or other item that poses an immediate and significant threat to public safety with little or no expectation of its recovery by the FBI.

### 13.2.2. (U) Tier I OIA Authorization

(U//FOUO) Tier I OIA requires advance written approval by the FO SAC. The CHS OIA sub-file must contain the authorization in accordance with subsection 13.9., "Recordkeeping Procedures."

(U//FOUO) In criminal investigations, the SA must contact (following the SAC's approval[6]) the FPO involved in the investigation to obtain the appropriate CFP authorization in writing. The AGG-CHS allow the SAC and CFP to agree to designate particular individuals at the supervisory level (i.e., ASAC) in their respective offices to carry out the approval functions assigned to them.

(U//FOUO) The appropriate CFP for all investigations except national security investigations is the CFP who:

- (U//FOUO) Is participating in an FBI investigation that is utilizing the CHS or working with that CHS in connection with a prosecution.
- (U//FOUO) Would have primary jurisdiction to prosecute the OIA that would violate a federal law.

OR

- (U//FOUO) Is located where the OIA is to occur.

(U//FOUO) For national security investigations or foreign intelligence collection, the CA must send, upon SAC approval, an EC to the appropriate FBIHQ operational unit to obtain AD

---

[5] (U) The citations to the USSG are to the 2005 edition. References to particular USSG sections are intended to remain applicable to the most closely corresponding USSG level in subsequent editions of the USSG in the event that the cited USSG provisions are amended. Thus, it is intended that the third bullet point of this subsection will remain applicable to the highest offense level in the Drug Quantity Table in future editions of the USSG, and that the fourth bullet point of this subsection will remain applicable to dollar amounts that, in future editions of the USSG, trigger sentencing enhancements similar to that set forth in the current section 2B1.1 (b)(1)(I). Any ambiguities in this regard should be resolved by the AAG for the Criminal Division.

[6] (U//FOUO) While the AGG-CHS only require SAC approval internally, current FBI practice for national security matters is to obtain FBIHQ operational AD approval after the SAC has approved the OIA, and then forward the approved request to the appropriate DOJ authority for its approval. The FO is not responsible for seeking DOJ approval in national security or foreign intelligence collection matters.

approval for the OIA, thereafter, the FBIHQ operational unit must forward the AD-approved request, in a document suitable for dissemination, to the appropriate DOJ authority for its approval. The FBIHQ operational unit must then notify the requesting FO, via EC, upon DOJ approval or denial of the request. A copy of the above OIA-related documentation must be filed in the CHS OIA sub-file.

(U//FOUO) The appropriate CFP for national security and foreign intelligence collection matters is the AAG of the DOJ NSD, or his or her designee. This designee may be an FPO attorney, however, the CHSC must verify that the delegation has taken place within the relevant FPO. If the CHSC is unable to identify an NSD designee, the FO should request assistance from the operational unit at FBIHQ.

(U//FOUO) As part of the approval process, the SAC and CFP authorizing Tier I OIA must make specific findings, set forth in subsection 13.4., "Documented Findings of Tier I and Tier II OIA Approvers," regarding the proposed illegal activity, which must be documented in the response to the OIA request. This documentation must be maintained in the CHS's OIA sub-file.

#### 13.2.2.1. (U//FOUO) CFP Authorization for Limited OIA Related to Material Support of Terrorism in National Security Investigations

(U//FOUO) For guidance on this authorization see DIOG subsection 17.6, "OIA Related to Material Support of Terrorism in National Security Investigations."

### 13.2.3. (U//FOUO) Tier I OIA Emergency Oral Authorization

(U//FOUO) Those authorized to approve Tier I OIA in accordance with subsection 13.2.2., "Tier I OIA Authorization," may orally authorize a CHS to engage in Tier I OIA without advance written documentation when they each determine that:

- (U//FOUO) A highly significant and unanticipated investigative opportunity would be lost if the OIA written authorization procedures were followed.
- (U//FOUO) These circumstances would support a finding to authorize the OIA pursuant to subsection 13.4., "Documented Findings of Tier I and Tier II OIA Approvers."

(U//FOUO) In such an event, the documentation requirements, including a written justification for the oral authorization, must be completed as soon as practicable, but within 72 hours following the oral approval in Delta.

### 13.2.4. (U) Tier I OIA Duration

(U//FOUO) Tier I OIA authorization must be set for a specified period not exceeding 90 days. An exception exists for national security investigations or foreign intelligence collection, for which the CFP may authorize OIA for a period of up to one year.

(U//FOUO) The Tier I OIA authorization period may be extended, according to the procedures set forth in subsection 13.6., "Renewal and Expansion of OIA Authorization."

## 13.3. (U) Tier II OIA

(U//FOUO) According to the AGG-CHS, Tier II OIA is any other activity that would constitute a misdemeanor or felony under federal, state, or local law if engaged in by a person acting without authorization.

### 13.3.1. (U) Tier II OIA Authorization

(U//FOUO) Tier II OIA requires the advance written approval (absent a request for emergency authorization in accordance with subsection 13.3.4., "Tier II OIA Duration") of the SAC. The authorization communication must contain specific findings regarding the proposed illegal activity, as set forth in subsection subsection 13.4., "Documented Findings of Tier I and Tier II OIA Approvers," and must be maintained in the CHS OIA sub-file. In states that require more than one-party consent to record communications, OIA authority must be requested in accordance with DIOG subsection 18.6.1.

### 13.3.2. (U) Coordination With FPO Attorney

(U//FOUO) FPO approval is not required for Type II OIA. However, if an FPO attorney is assigned to an investigation in which the CHS is assisting and the CHS is expected to testify, the CA must ensure that the FPO attorney is notified in advance of the OIA, if practicable. The OIA request must document the FO's written or oral notification in Delta.

### 13.3.3. (U) Tier II OIA Emergency Oral Authorization

(U//FOUO) In extraordinary circumstances, an SAC may orally authorize a CHS to engage in Tier II OIA, without advance documentation, after determining that a highly significant and unanticipated investigative opportunity would be lost if the FO were to follow the OIA written authorization procedures. In such an event, the SAC must complete the documentation requirements, including as written justification for the oral authorization, as soon as practicable, but within 72 hours. The CHS's OIA sub-file must document this approval communication.

### 13.3.4. (U) Tier II OIA Duration

(U//FOUO) Tier II OIA authorization must be set for a specified period not exceeding 90 days.

(U//FOUO) The Tier II OIA authorization period may be extended, according to the procedures set forth in subsection 13.6., "Renewal and Expansion of OIA Authorization."

## 13.4. (U) Documented Findings of Tier I and Tier II OIA Approvers

(U//FOUO) In accordance with subsection 13.2.2. and subsection 13.3.1. on OIA authorization, those authorized to approve Tier I and Tier II OIA must document in the CHS's OIA sub-file whether the benefits to be obtained from the CHS's participation in the illegal activity outweigh the risks involved and are necessary to either:

- (U//FOUO) Obtain information or evidence that is essential for the success of an investigation and is not reasonably available without such activity, including illegal activity to maintain the CHS's credibility and thereby obtain the information or evidence.

OR

- (U//FOUO) Prevent death, serious bodily injury, or significant damage to property.

(U//FOUO) In making these findings, the approvers must consider:

- (U//FOUO) The importance of the investigation.
- (U//FOUO) The likelihood of obtaining the information or evidence.
- (U//FOUO) The risk of the CHS misunderstanding or exceeding the scope of his or her authorization.

- (U//FOUO) The extent of the CHS's participation in the OIA.
- (U//FOUO) The risk of the FBI being unable to monitor the CHS's participation in the OIA.
- (U//FOUO) The risk of violence, physical injury, property damage, or financial loss to the CHS or others.
- (U//FOUO) The risk of the FBI being unable to ensure that the CHS does not realize undue profits from his or her participation in the OIA.

### 13.4.1. (U) Precautionary Measures

(U//FOUO) Whenever an SA has obtained authorization for a CHS to engage in OIA the SA must take all reasonable steps to:

- (U/FOUO) Monitor the activities of the CHS closely
- (U//FOUO) Minimize the adverse affect of the OIA on innocent persons; and
- (U//FOUO) Ensure that the CHS does not realize undue profits from his or her participation in the OIA.

## 13.5. (U) Admonishments Related to OIA

(U//FOUO) If a CHS is authorized to engage in OIA, two SAs—or one SA and one government official as a witness—must review written admonishments with the CHS that state, at a minimum, that:

- (U//FOUO) The CHS is authorized to engage only in the specific conduct set forth in the written authorization, and not in any other illegal activity (the CFP's written authorization should be read to the CHS, unless doing so is not feasible).
- (U//FOUO) The CHS's authorization is limited to the time period specified in the written authorization.
- (U//FOUO) Under no circumstance may the CHS:
  - (U//FOUO) Participate in an act of violence (except in self-defense).
  - (U//FOUO) Participate in an act designed to obtain information for the FBI that would be unlawful if conducted by an LE agent (e.g., breaking and entering, illegal wiretapping, illegal opening or tampering with the mail, or trespass amounting to an illegal search).
  - (U//FOUO) If applicable: participate in an act that constitutes obstruction of justice (e.g., perjury, witness tampering, witness intimidation, entrapment, or the fabrication, alteration, or destruction of evidence).
  - (U//FOUO) If applicable: initiate or instigate a plan or strategy to commit a federal, state, or local offense.
- (U//FOUO) If the CHS is asked by any person to participate in any illegal activity other than the specific conduct set forth in the written authorization, or learns of plans to engage in such illegal activity, the CHS must immediately report the matter to the FBI CA or co-CA.

- (U//FOUO) Participation in any illegal activity other than the specific conduct set forth in the written authorization could subject the CHS to criminal prosecution.

(U//FOUO) Immediately after receiving these admonishments, the CHS must use his or her payment name to sign (or initial) and date a written acknowledgment of the admonishments (see subsection 16.3., "Payment Name"). If the CHS refuses to sign or initial this acknowledgment, the SA and witness who presented the admonishments must document that these admonishments were reviewed with the CHS and that the CHS acknowledged his or her understanding of them. An SSA must review the OIA admonishment documentation and ensure that it is maintained in the CHS's OIA sub-file (see subsection 13.9., "Recordkeeping Procedures").

### 13.6. (U) Renewal and Expansion of OIA Authorization

(U//FOUO) If an agent seeks to reauthorize any CHS to engage in OIA after the expiration of the authorized time period or revocation of authorization or to expand, in any material way, a CHS's authorization to engage in OIA, the requesting agent must first comply with the procedures set forth in subsection 13.2.2. ("Tier I OIA Authorization") or 13.3.1. ("Tier II OIA Authorization") and subsections 13.4. ("Documented Findings of Tier I and Tier II OIA Approvers") and 13.5. ("Admonishments Related to OIA").

### 13.7. (U) Suspension of OIA Authorization

(U//FOUO) Whenever an SA cannot comply with the precautionary measures described above for legitimate reasons that are unrelated to the CHS's conduct (e.g., the CA is unavailable), the CA must immediately:

- (U//FOUO) Suspend the CHS's authorization to engage in OIA until the SA can comply with the precautionary measures.
- (U//FOUO) Inform the CHS that his or her authorization to engage in any OIA has been suspended until that time.
- (U//FOUO) Document these actions in the CHS OIA sub-file.

### 13.8. (U) Revocation of OIA Authorization

(U//FOUO) If an SA has reason to believe that a CHS has failed to comply with the terms of the OIA authorization, the agent must immediately:

- (U//FOUO) Revoke the CHS's authorization to engage in OIA.
- (U//FOUO) Inform the CHS that he or she is no longer authorized to engage in any OIA.
- (U//FOUO) Comply with the notification requirement described below.
- (U//FOUO) Determine whether the CHS should be closed pursuant to Section 18., "Closing a Confidential Human Source."
- (U//FOUO) Document these actions in the CHS OIA sub-file.

(U//FOUO) Immediately after the CHS has been informed that the individual's authorization to participate in OIA has been revoked, the CHS must use his or her payment name to sign and date a written acknowledgment that he or she has been informed of this fact. If the CHS refuses to sign the acknowledgment, the SA who informed the CHS must document the CHS's refusal and whether the CHS verbally acknowledged receipt of the revocation. The SSA must review this

OIA revocation documentation as soon as practicable and ensure that it is placed into the CHS's OIA sub-file.

### 13.9. (U) Recordkeeping Procedures

[redacted]

# 14. (U//FOUO) Operation of Confidential Human Sources Involving Other Federal, State, Local, and Tribal Agencies or FBI Field Offices

## 14.1. (U) Joint Operations of FBI CHSs With Other Agencies

(U//FOUO) Joint operation of a CHS takes place when the FBI and one or more other agencies operate an FBI CHS together in a matter of mutual interest to all agencies involved. CHS operations, while joint, must comply with applicable AGGs and FBI policy.

### 14.1.1. (S//NF) Joint Operation With CIA, USG, OR USIC to Advance National Security Objectives

(S//NF) The CA or co-CA must advise the [redacted] by completing and forwarding the [redacted] of any joint CHS operation with the CIA, USG, or USIC when the purpose of the joint operation is to render intelligence or other specific support to advance USG national security objectives. That communication will serve to document the agencies' agreement regarding their responsibilities for the joint CHS operation. The agreement should be consistent with each agency's policy and any existing interagency agreements. Areas to address may include the establishment of the lead agency for the relevant operational period (especially if the CHS will be operated in a foreign country), validation, tasking, debriefing, funding, communications plans, documentation of reporting, and intelligence sharing and dissemination. [redacted]

## 14.2. (U) Sole Operation of an FBI CHS by Another Agency

(U//FOUO) The sole operation of a CHS by another agency occurs when an FBI CHS is temporarily turned over to another agency for operation in a matter of exclusive interest to that agency. The FBI, however, must relinquish responsibility for the CHS to the other agency and have no role in tasking, paying, or contacting the CHS in connection with the other agency's investigation.

(U//FOUO) In order for an FO to turn over a CHS to another agency for sole operation by that agency, the CA or co-CA must submit a request for SSA approval that includes the following information: the name of the agency, the name of the agency employee who will handle the CHS, the nature of the case in which the CHS will be used, and the anticipated duration of the operation. In view of the potential liability concerns of maintaining the CHS in open status, the CHS must be closed while being operated by the other agency. In rare circumstances, such as those that involve the CHS's intelligence value or potential to assist other FBI operations, the CHS may remain open for up to six months while being operated solely by the other agency. During the period the CHS remains open, all administrative requirements must be performed, including Quarterly Supervisory Source Reports (QSSRs), FOASRs, annual records checks, and annual admonishments. In conducting the QSSRs, the SSA must evaluate the nature and duration of the CHS's use by the other agency, and determine whether the use is negatively affecting the CHS's use to the FBI, to the extent that the CHS should be closed. Although the FBI is not responsible for validating the CHS's information or operation during the period the CHS is out of the FBI's control, the CA must make reasonable efforts to periodically (at least every 90 days)

obtain information from the other agency regarding CHS payments and any information the other agency can provide bearing on the CHS's productivity, reliability, and credibility. This information must be documented in the CHS's validation sub-file.

### 14.3. (U//FOUO) Joint Field Office Operation or a CHS Operating Within Another FBI Field Office

(U//FOUO) A CHS may work jointly with two or more FBI FOs. If the CHS resides in, moves to, or works in another FO's territory, the office of origin (OO) must notify the SAC (or designee) and all other involved FOs of the CHS's opening; the OO must also notify the FOs of the area of anticipated reporting, and the notification must be documented in the CHS Delta file. The CA and co-CA may be located in different offices if it will enhance the CHS' operational effectiveness. The OO is responsible for maintaining the CHS file, and if the CHS is jointly operated, the other FOs involved in operating the CHS must file all reports of information received from the CHS, as well as any required documentation (e.g., payment information and receipts), to the OO file. Similarly, both offices must keep the other apprised of information affecting the FO's investigative programs and any changes in the CHS's status. To make a payment to a CHS on behalf of another FO, see subsection 17.9., "Paying a CHS."

(U//FOUO) In situations where the OO has temporarily turned over a CHS to another FO for operational use in that FO's investigation, the FO using and tasking the CHS is responsible for ensuring that all communications pertaining to the CHS's operation (e.g., reporting, operational requests, payment documentation, and validation-related information) are promptly entered into Delta. CHS payments made by another FO are addressed in subsection 17.12., "Payments to CHSs by Other Field Offices." The FO tasking the CHS must also keep the OO advised of any information it obtains from the CHS that would affect the OO's investigative programs. During the other FO's operation of the CHS, the FO tasking the CHS must contribute to the OO's preparation of the CHS QSSRs and FOASRs and ensure compliance with other administrative requirements, including annual records checks and admonishments. If the other FO tasking the CHS has used the CHS exclusively for a six-month period and is likely to continue this use, the OO must reassign the CHS to the other FO.

### 14.4. (U//FOUO) Operation of CHSs in Another Field Office's Territory

(U//FOUO) This subsection concerns CHS domestic-operational travel, in which a CHS travels from one FO AOR to another FO AOR or from a foreign country to the United States to conduct operational activity. This type of travel includes, for example a CHS traveling from his or her assigned FO to another FO to support an investigation; a Legat-assigned CHS traveling to the United States to support an FO investigation; or an FO-assigned CHS who resides in a foreign country traveling to the United States in support of an investigation. See subsection 19.4.1.5., "Foreign-Based CHS Operational Travel to United States (Domestic-Operational Travel)."

(U//FOUO) An SA seeking to conduct a CHS operation in another FO's territory must obtain prior concurrence from the SAC (or designee) of the other FO in which the operation will occur, if practicable. If not practicable, the affected FO(s) must be notified as soon as possible, but no later than five business days from the date of the operational activity. The [redacted] "CHS Travel/ET Activity Request Form," should be used to document the prior concurrence or post-operation notification of the affected FO(s). If the form is used, an information-only lead is sent to the receiving FO for situational awareness. The use of the [redacted] does not preclude informal oral or written contact between FOs to coordinate the CHS activity.

Regardless of whether or not the [redacted] is used, the CHS's domestic operational travel must be documented in the CHS file.

(U//FOUO) The above provision does not apply to online operations. For CHS online operational activity known to affect another FO's AOR, coordination between affected FOs is recommended for deconfliction purposes. Coordination efforts must be documented in the CHS main file.

# 15. (U//FOUO) Disclosure of a Confidential Human Source's Identity

## 15.1. (U) Principles of Confidentiality

(U//FOUO) Protecting a CHS's identity and relationship with the FBI is vital to the success of that relationship and to the integrity of the FBI's CHS program. Consequently, FBI personnel have an obligation to maintain the confidentiality of any CHS, which includes the CHS's identity and information received from or regarding the CHS that tends to identify the CHS. This obligation continues after the FBI employee ends his or her employment and after the CHS ceases to be a CHS.

(U//FOUO) Disclosure of a CHS's identity, which includes the dissemination of information received from or regarding the CHS that tends to identify him or her, should be approved only when it is legally required or absolutely necessary to achieve important investigative, public policy, or safety objectives. This principle must be at the forefront of every disclosure decision, even with regard to prospective disclosures within the DOJ and among task force partners.

## 15.2. (U) Disclosure Authority

(U//FOUO) Approval of the SAC from the office where the CHS is assigned is required to disclose the identity of a CHS, unless:

- (U//FOUO) FBI personnel disclose a CHS's identity to another FBI employee who has a need to know the identity of the CHS to perform his or her official duties.
- (U//FOUO) FBI personnel make appropriate disclosures to the DOJ when a CHS has been called to testify in a grand jury or judicial proceeding.
- (U//FOUO) FBI personnel disclose a CHS's identity when required to do so by court order, law, regulation, the AGG-CHS, or other DOJ policies (see, for example, subsection 11.7., "Responding to Requests from FPO Attorneys Regarding a CHS").

(U//FOUO) The SSA may approve the disclosure of a CHS's identity in response to operational or administrative requests that by their nature require disclosure of a CHS's identity, including those related to surveillance plans, arrest plans, requests for linguistic support, joint operations of CHSs, NFPO requests, requests to DHS for immigration status, and requests for DOS information. Prior to approving a disclosure request, the SSA, in discussion with the CA, should consider the necessity of disclosing the CHS's identity, its potential for undermining the confidential relationship developed, and whether the CHS should be informed that his or her identity will be shared as part of an operational or administrative request. SSA approval of the specific operational or administrative request serves as the authorization documentation to disclose the CHS's identity. No separate documentation is required for disclosing the CHS's identity in such circumstances.

(U//FOUO) No individual to whom disclosure has been made is authorized to make further disclosures of the CHS's identity without SAC authority, except when required by court order, law, regulation, the AGG-CHS, or other DOJ policies. Anyone making a disclosure has the responsibility to advise the recipient of the information that further disclosures or contact with the CHS is not authorized without the express consent of the FBI.

(U//FOUO) All approvals to disclose CHS identity must be documented in the CHS main file.

### 15.3. (U//FOUO) SAC Objection to CHS Disclosure Requirement

(U//FOUO) With regard to a required disclosure, the SAC may still determine whether an attempt should be made to assert appropriate administrative or legal objections in response to any subpoena, court order, or request bearing on the identification of a CHS. In matters involving national security and other situations, a request may be made to have the CHS's file reviewed in camera ex parte by a judge, as appropriate. In certain circumstances, the FBI may refuse the disclosure of either the CHS's identity or information provided by the CHS. This action could result in the dismissal of the pending prosecution and must be coordinated with appropriate officials from the FPO. Any decision to withhold CHS information must be coordinated with the appropriate FPO and documented in the CHS's main file.

### 15.4. (U//FOUO) Record of Disclosure of CHS Identity

(U//FOUO) Disclosure of a CHS's identity or relationship with the FBI, as fined above, must be documented and retained in the CHS's file. The documentation must contain the following information:

- (U//FOUO) The specific information to be disclosed (e.g., the CHS's name and address)
- (U//FOUO) The name, title, and agency or department of all individuals who will have access to the information
- (U//FOUO) The specific nature of the circumstances, request, demand, or order that generated the disclosure request

(U//FOUO) The SSA approval of a specified operational or administrative request serves as the authorization documentation to disclose the CHS's identity. No separate documentation is required. See subsection 15.2., "Disclosure Authority."

# 16. (U//FOUO) Administration of Confidential Human Sources

## 16.1. (U//FOUO) CHS Files

### 16.1.1. (U//FOUO) Creation and Maintenance of CHS Files in Delta

(U//FOUO) Delta is the FBI's automated case management system for all CHS records. All communications regarding the CHS must be entered into Delta, unless an exemption is authorized in accordance with subsection 16.1.2., below.

[redacted]

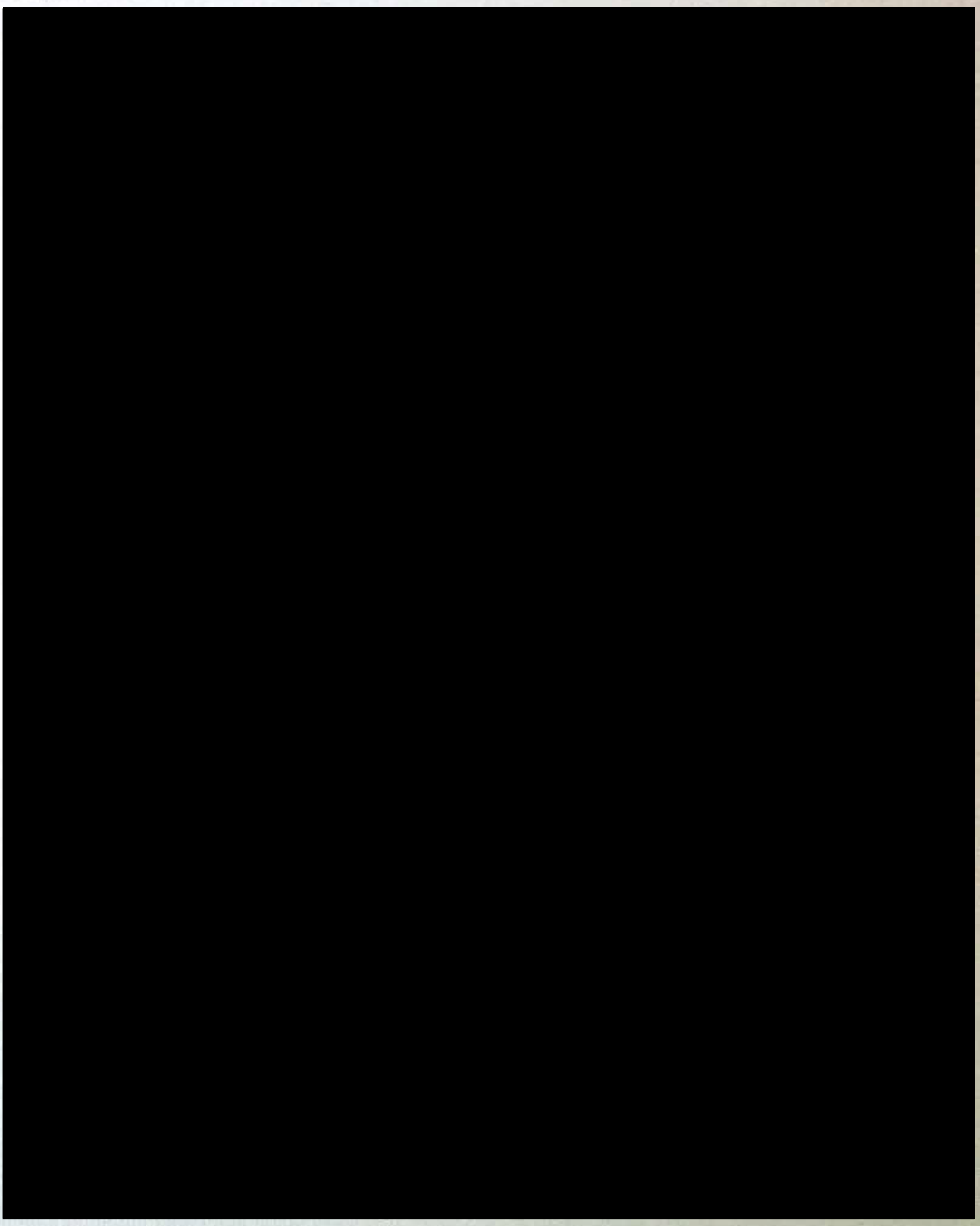
### 16.1.2. (U//FOUO) Exemption From Creation and Maintenance of CHS Files in Delta

(U//FOUO) Exemptions from entering communications into Delta must be supported by compelling circumstances and approved by the SAC, the AD of the division managing the primary program the CHS supports, the AD of the DI, and the Deputy Director (DD). None of these approving authorities may be delegated. An EC requesting a Delta use exemption must utilize [redacted] and must provide the following, without providing any CHS identifying or classified information (additional guidance on completing the request EC may be sought from [redacted]):

- (U//FOUO) What information is to be exempted from entry into Delta
- (U//FOUO) Why entry of this information into Delta would likely compromise the CHS or jeopardize the investigation due to:
  - (U//FOUO) Sensitivity of the CHS.
  - (U//FOUO) Singularity of the information the CHS is providing.
  - (U//FOUO) Degree to which the CHS information is critical to the success of the investigation.
- (U//FOUO) How entry of the information will:
  - (U//FOUO) Cause immediate harm to the national security of the United States.
  - (U//FOUO) Cause harm to the FBI's ability to recruit and operate other CHSs of similar circumstances.
  - (U//FOUO) Impede the FBI's ability to collect for both the FBI's and the USIC's intelligence requirements.
- (U//FOUO) How intelligence collected from the CHS will be evaluated and disseminated to other FBI components or outside the FBI that is critical to the FBI's mission, such as thwarting a terrorist attack or other national emergency

(U//FOUO) The EC must set a lead to [redacted] requesting DD approval for the exemption request. [redacted] is responsible for notifying the CA of the approval or denial of the request. If the request is approved, [redacted] is responsible for permitting the CA or co-CA to initiate the opening of the CHS, including the limited submission required for Delta, as specified below.

(U//FOUO) Upon receiving the DD's approval, the CA or co-CA must complete all mandatory fields in the Delta source-opening communication so that the CHS can be opened in Delta (in order for the CHS to be paid) and to ensure that the QSSR and FOASR are accurately completed. However, to protect the CHS's identity, the [redacted] has created standardized responses to be entered into each field by the CA or co-CA. The following is a list of the mandatory fields and the responses to be entered:



- (U//FOUO) Co-Case Agent
  - (S//NF) Enter accurate information
- (U//FOUO) CHS Assessment (Section III)
  - (S//NF) Enter "NO" for all questions

### 16.1.3. (U//FOUO) Opening the CHS on Paper, For Delta Exempt

(U//FOUO) To open the CHS on paper, the CA or co-CA must—after registering the CHS in Delta—complete a full, accurate source-opening communication using the "Opening EC" template located on [redacted]. The CA or co-CA must ensure that all appropriate leads are set and disseminated via hard copy to [redacted]. In addition, the "s" number assigned to the CHS when he or she was registered in Delta must be listed in the title of the EC.

### 16.1.4. [redacted]

[redacted]

### 16.1.5. (U//FOUO) CHS File Structure and Content

(U//FOUO) The CHS main file contains all the personal and administrative information about the CHS (e.g., criminal history, AUSA letters, and background database checks) [redacted]

- [redacted]

(U//FOUO) Information not reported on a Delta form (e.g., receipts, photographs, computer printouts, handwritten notes, consent forms) must be scanned, if possible, and uploaded into the appropriate file or sub-file. Information or physical items that cannot be scanned (e.g., a gift) must be maintained in the 1A section of the CHS file [redacted]

[redacted]

### 16.1.6. (U) Properly Classifying CHS Information

(U//FOUO) If a CHS's background information or the information he or she reports reflects matters of national security requiring classification, that information must be appropriately classified in accordance with the *National Security Information Classification Guide* (NSICG). This guide specifies, among other information that must be classified, the following:

- (U//FOUO) CHS-2 information provided by a CHS on matters pertaining to national security that allows a reasonable inference of the identity of the source
- (U//FOUO) CHS-3 information provided by a CHS on matters pertaining to national security that does not allow a reasonable inference of the identity of the source

(U//FOUO) All classified information [redacted]

(U//FOUO) Any information with a classification level above SECRET must be referenced in Delta via a general-purpose insert denoting the location of the higher-classified reporting or information. Until an appropriate tool exists for electronic storage, the hard-copy document must be retained in a secure location.

### 16.1.7. (U) Documenting CHS Information

(U//FOUO) Information provided by a CHS that is testimonial in nature or has intelligence value must be documented on a CHS reporting document in a way that does not identify the CHS; it must be maintained separately from the CHS's personal information and the information the CA provided to the CHS to complete taskings.

(U//FOUO) CHS reporting documents must not refer to the CHS by payment name or code name. The documents must be appropriately classified [redacted] in the appropriate classified or unclassified sub-file and appropriate operational case or intelligence files. [redacted]

(U//FOUO) Information provided by the CHS that is not intelligence or testimonial in nature must be documented in a CHS contact report and maintained in the validation sub-file. A contact report is used to document following:

- (U//FOUO) The CA's observations of the CHS
- (U//FOUO) Disclosures of information to the CHS in connection with a tasking, including any documents given to the CHS
- (U//FOUO) Personal information regarding the CHS, including the CHS's finances, health problems, major life changes, and anomalies (e.g., changes in the CHS's demeanor or behavior)
- (U//FOUO) Any derogatory information received from other CHSs
- (U//FOUO) Topics discussed with the CHS, including any topics initiated by the CHS
- (U//FOUO) Each person present for the meeting with the CHS
- (U//FOUO) Other information that may affect the CHS's reliability or credibility

(U//FOUO) Both the CHS reporting document and the contact report must be uploaded into Delta within five business days of contact with the CHS.

### 16.1.7.1. (U) Dissemination of CHS Reporting

(U//FOUO) This subsection addresses the dissemination of CHS reporting that does not tend to identify the CHS. The dissemination of CHS reporting that tends to identify the CHS is treated as a disclosure of the CHS's identity and is addressed in Section 15, "Disclosure of a Confidential Human Source's Identity."

(U//FOUO) The dissemination of CHS reporting is encouraged and should be made available to members of LE, the IC, or tribal authorities with proper clearance if it is within the scope of their mission (see DIOG, Section 14). Disseminations are made through an intelligence information report (IIR) or other documents created for the purpose of sharing information (e.g., an LHM, an intelligence assessment, an intelligence bulletin, or similar). For documents not created for the purpose of dissemination, such as an [redacted] CHS reporting must be closely reviewed prior to dissemination and redacted to protect the identity of the CHS, unless the disclosure of his or her identity is justified and authorized in accordance with subsection 15.2., "Disclosure Authority."

(U//FOUO) Whichever dissemination method is used, the CA must document the dissemination of CHS reporting, including:

- (U//FOUO) The name of the person to whom and/or agency to which the information was disclosed.
- (U//FOUO) A description of the information disclosed.

(U//FOUO) The dissemination record must be maintained in the CHS's file and can be a copy of the disseminated document (e.g., a copy of the [redacted], IIR, or LHM). The dissemination must also be claimed as a statistical accomplishment on the source contact report [redacted], noting the file and serial number of the disseminated information or a description of the information that was disclosed. If the information was disseminated in an IIR, the IIR number should be referenced on the source contact report. In addition, dissemination from the CHS file should be documented in the FOASR.

(U//FOUO) If the CHS's reporting was used in a court document, that fact must be claimed as a statistic on the source contact report if the activity meets the threshold for claiming an accomplishment. If the CHS testifies in a court proceeding, claiming a statistical accomplishment on the source contact report is sufficient documentation. For reporting at levels higher than SECRET, the electronic file location must be noted in the Delta file.

### 16.1.8. (U) Retention of CHS Files

(U//FOUO) The National Archives and Records Administration (NARA) has designated CHS files for permanent retention. Therefore, records relating to CHSs must not be deleted or destroyed.

### 16.2. (U//FOUO) CHS Number

(U//FOUO) When a CHS file is opened in Delta, the CHS is assigned an "S" (symbol) number, which serves as the CHS file number. This number may also be used to identify the CHS in communications sent to other government agencies (OGAs) and in internal FBI documents. The S number must not, however, be disclosed to the CHS.

### 16.3. (U) Payment Name

(U//FOUO) An SA must assign a payment name to a CHS to enable the CHS to sign documents such as payment receipts, OIA admonishments, a service agreement, and consensual monitoring consent forms in a covert manner. The payment name must be unique within the FO. It may contain both letters and numbers, but must not indicate the CHS's true identity. The assignment of the payment name must be documented in the CHS's main file. The payment name should not appear in any disseminable document except for communications to DOJ.

### 16.4. (U) Code Name

(S//NF) Code names may be used for CHSs who are DAs, non-DAs in joint operations, defectors, RIPs, or unusually sensitive CHSs, and they should be obtained from the appropriate [redacted] unit's code name/code word database. Codenames must be unique to the CHS and previously unused within the FBI.

### 16.5. (U//FOUO) CJIS Division/NCIC "Stop Notices"

(U//FOUO) When the opening communication for a new or reopened CHS is completed and approved, the appropriate [redacted] unit must notify CJIS to place a query alert notification (QAN, previously known as a "stop notice"). CJIS will flag the CHS record using biographical and/or biometrics information. When an NCIC inquiry is made on the CHS, this QAN automatically triggers a notification to CJIS, and CJIS in turn will notify the FO of the inquiry. The CA has an obligation to ascertain the basis of the NCIC inquiry and take whatever action may be necessary to resolve it. The QAN will be placed in the main folder of the CHS file in Delta; when a CHS is closed, CJIS will cancel the QAN on the CHS.

### 16.6. (U) Positive Records Checks and Concurrence to Operate

(U//FOUO) If a records check determines that a CHS is the subject of an ongoing FBI investigation, the CA attempting to open the person must first obtain the concurrence of the FO SSA conducting the investigation. The concurrence must be documented in the CHS's main file. If the CHS has outstanding criminal charges, the CA must contact the issuing agency. If the jurisdiction with the outstanding charges is not willing to extradite, then the CA must document that fact, and the individual may be opened as a CHS. For guidance on fugitives, see subsection 7.13., "Fugitives." In addition, an FPO may have to be notified (see subsection 11.3., "Notification to DOJ of the Investigation or Prosecution of a CHS").

### 16.7. (U) Field Office Annual Source Report

(U//FOUO) The FOASR is the FO executive management's review of the CHS file. The FOASR is a critical tool used to assess the CHS for continued operation. The CA must provide detailed information regarding the CHS relevant to each topic and question in the FOASR. A thorough and complete FOASR enables the SSA, ASAC, and FBIHQ to accurately assess the CHS's operation and provides subsequent handlers with all information pertinent to the continued operation of the CHS. The ASAC is responsible for ensuring that squads fulfill their validation

duties according to the standards set forth in this section. In addition, ASACs are responsible for the completion and submission of the FOASR by the due date. The ASAC cannot further delegate this responsibility.

(U//FOUO) The CA must complete the FOASR in Delta annually, based on the date of opening for the CHS. The FOASR must be approved by the SSA and ASAC. The final approver must submit the FOASR via Delta within 30 days of this anniversary date. If the CA is unavailable to complete the FOASR, the co-CA (who is an FBI SA and not a TFO) must complete the FOASR. If no co-CA is available, the SSA must ensure that the FOASR is completed in order for the FO to remain in compliance.

### 16.8. (U) Quarterly Supervisory Source Report

(U//FOUO) The SSA must prepare a QSSR for each consecutive 90-calendar-day period for each CHS file assigned to the SAs under the SSA's supervision. The initial 90-day period calculation starts on the CHS file opening date. The SSA must complete the QSSR review within 30 calendar days of the end of the CHS's 90-day cycle. The SSA must review all sub-files for each CHS, including specifically the Sub V (validation) file, to note any significant anomalies (e.g., potential derogatory information about the CHS, sudden and constant requests for money, contact information indicating substantial change in behavior, lifestyle or viewpoint on issues of past importance) that occurred in the last 90 days. If anomalies exist, the SSA must document what action has been taken with respect to addressing the anomalies or explain why no action is necessary. In addition, the SSA must consult with the ASAC regarding the anomalies, and the ASAC's concurrence with the SSA's course of action must be documented in the QSSR. An acting SSA may not conduct a QSSR of his or her own CHS file. The acting SSA's ASAC is responsible for conducting the QSSR of the acting SSA's CHS file.

### 16.9. (U) Annual Database Checks

(U//FOUO) The FO must conduct queries of FBI universal indices, ELSUR, and criminal history on an annual basis, as measured from the CHS file opening date. Other database checks (e.g., FinCEN, TECS, or civil court records) may also be conducted annually, if applicable to their reporting. All queries and their results, including derogatory information, must be documented in the CHS's main file and noted on the FOASR.

### 16.10. (U) Documenting CHS Derogatory Information

(U//FOUO) If an FBI employee receives derogatory information on an individual whom he or she reasonably believes to be an open CHS, the FBI employee must request that the CFR staff conduct a Delta query on the name of that person to determine whether the person is a CHS. If the person is identified as a CHS, the query will alert the agent assigned to the CHS to address the query with the agent requesting the search. The assigned CA agent must then document the information received to the validation sub-file.

### 16.11. (U) Other CHS-Related Deconfliction Checks

(U//FOUO) A TFO or an SA may request the CHSC or CFR staff in his or her respective FO or division to conduct a check of CHS databases, including legacy CHS files, to determine whether an individual is currently or was previously an FBI CHS. The request must be in writing (e.g., an EC or a record e-mail) and have prior approval from the SSA of the requesting TFO or SA. The SSA must evaluate the request to ensure that sufficient justification exists to search FBI CHS files and that the request is not capricious or an improper use of resources. The SSA must also

ensure that the request is rationally related to a national security or criminal activity purpose. If the request is approved and there is a positive result, the CHSC, in coordination with the assigned CA (if any), must disclose to the requestor only the CHS-related information that is necessary to support the request's justification. The approved requesting document and any information disclosed on a CHS must be maintained in the CFR and filed into the CHS file. If a search yields a negative result, the requesting document must be maintained in the CFR program control file related to CHS administration.

### 16.12. (U//FOUO) Transport of CHS Files and Access to Delta Files by Another Field Office or FBIHQ

(U//FOUO) Physical possession of a CHS's original paper file must never be transferred to any individual outside the FBI, unless it is done pursuant to a court order or in order for a federal judge to conduct an in-camera ex parte review. In these cases, the file must be transported by an SA.

(U//FOUO) Should FBIHQ or an FO require another FO's original CHS file, in whole or in part, the file may be sent by FBI-approved carriers to the office requesting the file, with SAC approval. This process includes common carriers and methods approved for shipping classified FBI information. For access to open CHS files in Delta, the requesting SA must make a request to the CHS's CA. When access is granted by the CA, the OO's CHSC will create the appropriate role for the SA requestor.

(U//FOUO) SAC approval is not required for requests for the original CHS file from Validation Section (VS) employees handling CHS validation matters, and FOs are required to send the requested information. See Section 20, "Confidential Human Source Validation," for additional guidance.

16.13. [redacted]

[redacted]

# 17. (U//FOUO) Confidential Human Source Financial Matters

(U//FOUO) The FBI may compensate a CHS for services provided and/or reimburse his or her expenses incurred in furtherance of an investigative matter, including those occurring in a foreign country. All CHS payments are subject to FBI audit procedures. [redacted]

(U//FOUO) All CHS payment requests must be submitted through Delta via the [redacted], "Payment Request," and recorded in the Delta CE (case expenditures) sub-file. Payment documents containing the CHS's true name must be filed in the Delta main file, with redacted copies sent to the CE sub-file. Upon payment, all CHS payments must be immediately reconciled with payment requests in Delta.

(U//FOUO) Certain fiscal circumstances require DOJ exemptions from statutes that would otherwise prohibit the activities. The fiscal circumstances are delineated in the AGG-UCO. However, the applicable statutes and the requirement for a DOJ exemption apply even if the operation is a CHS operation and not a UCO.

(U) The following fiscal circumstances require exemptions:

- (U//FOUO) The deposit of appropriated funds in banks or other financial institutions
- (U//FOUO) The purchase of real property or the lease of space
- (U//FOUO) The use of project-generate income (PGI) to offset necessary and reasonable expenses incurred

(U//FOUO) See the [redacted] section on fiscal circumstances for additional details. This policy guide is used only as reference for the parameters and procedure for seeking DOJ exemptions.

## 17.1. (U) Payment Prohibitions

(U//FOUO) Under no circumstances may any payments to a CHS be contingent upon the conviction or punishment of any individual.

(U//FOUO) In determining the way to classify a particular payment to a CHS as a service or an expense, the CA should not consider whether or not that classification might result in a basis for an impeachment at trial.

## 17.2. (U//FOUO) Field Office Funding for CHSs

(U//FOUO) FO funding allocations for CHSs supporting programs in the Counterterrorism, Counterintelligence, Weapons of Mass Destruction, Criminal Investigative, and Cyber Divisions are managed by the operational desks and budget units in those divisions. CHS budgetary enhancement requests relating to those programs should be submitted to the appropriate operational desk or budget unit. Funding allocations relating to CHSs supporting the Intelligence Program are managed by the appropriate [redacted] unit.

## 17.3. (U) SAC Annual CHS Payment Authority

(U//FOUO) The SAC has a payment authority of $100,000 per FY for each CHS. This authority is automatically renewed to $100,000 at the beginning of each FY. In the event that the payment authority of $100,000 is expended prior to the end of the FY, the FO may request enhanced

payment authority of $100,000. An amount exceeding $100,000 may be requested if that amount is justified by operational considerations.

(U//FOUO) A request for enhanced SAC payment authority must include the following information:

- (U//FOUO) The CHS's S number
- (U//FOUO) The dollar amount of the additional payment authority requested
- (U//FOUO) Supporting justification for the amount requested

(U//FOUO) The request EC must be approved through the FO SAC and serialized in the [redacted] sub-file using the two- or three-letter sub-file designation of the FO or FBIHQ unit with primary responsibility over the program the CHS reports on. The CA should not use any identifying information of the CHS and should only identify the CHS by Delta S number. Although [redacted] and all sub-files are restricted, the CA must use appropriate caution so as not to reveal the identity of the CHS in the body of the EC.

(U//FOUO) The request EC must include an action lead to the operational unit responsible for the oversight of the cases on which the CHS is reporting. The action lead must request FBIHQ approval (according to the approval levels set forth below) to continue to utilize and pay the identified CHS. The operational unit must review the operational benefits gained from previous payments to the CHS and evaluate the operational benefits likely to be gained if the enhanced payment authority is approved.

(U//FOUO) The operational unit must advise the requesting FO and [redacted] of the approval or denial of the enhanced payment authority in accordance with the above guidance. The operational unit must document its decision to approve or deny the FO's request in an EC to the FBIHQ and [redacted] sub-files. The EC must contain a lead set to [redacted] notifying [redacted] of the approval or denial. The FO may not make any additional payments to the CHS until the FBIHQ operational unit has advised that authority has been granted for continued payment. The FO must also maintain the approval/denial response EC in the CHS CE sub-file.

(U//FOUO) The EC generated by the operational unit for approval or denial of the enhanced payment authority must be signed at the approval level appropriate for the amount of the request, as follows:

- (U) Authority to exceed the annual payment authority threshold of $100,000 and pay up to $200,000 within the FY requires operational DAD approval.
- (U) Authority to pay a CHS between $200,000 and $300,000 within the FY requires operational AD approval.
- (U) Authority to pay a CHS between $300,000 and $400,000 within the FY requires operational AD approval.
- (U) Authority to pay a CHS between $400,000 and $500,000 within the FY requires operational branch EAD approval.
- (U) Authority to exceed the $500,000 threshold and each $100,000 increment above $500,000 requires DD approval.

(U//FOUO) Delegated authorities within the operational divisions must be documented in advance to the appropriate operational division sub-file, as directed in DIOG subsections 3.4.3.3.1 and 3.4.3.3.2.

### 17.4. (U) Aggregate Payment Authority

(U//FOUO) When the FBI's total expense and/or service payments to a CHS over the lifetime use of that CHS reach $100,000, and at increments of $100,000 thereafter (i.e., $200,000, $300,000, $400,000, and so on), the FO must request authority for the continued payment of the CHS up to the next $100,000 incremental threshold. All requests for authority to continue to pay the CHS, based on aggregate payments, must include:

- (U//FOUO) The CHS's S number.
- (U//FOUO) Total services vs. expenses paid, by case, along with a brief justification for those payments. The justification should be detailed enough to allow for a determination of payments vs. CHS contributions.
- (U//FOUO) Supporting justification for the continued payment of the CHS up to the next $100,000 incremental threshold.

(U//FOUO) The request EC must be serialized in the [redacted] sub-file, using the two- or three-letter sub-file designation, to both the FO and the FBIHQ operational unit.

(U//FOUO) The request must be approved by the SAC in an EC with an action lead to the FBIHQ operational unit responsible for the oversight of the cases on which the CHS is reporting. The EC must also contain an information lead to the appropriate unit in the [redacted] (currently [redacted] to ensure the availability of future payments via Delta if the request is approved. The operational unit must review the operational benefits gained from the previous payments to the CHS and evaluate the importance and operational benefits likely to be gained if the enhanced payment authority is approved.

(U//FOUO) The FBIHQ operational unit must obtain, via EC, approval or denial of the request from the appropriate FBIHQ approving official listed below. The same EC must also advise the FO and notify the appropriate DI unit of the FBIHQ official's decision to approve or deny the FO request, using the [redacted] sub-files. The requesting FO must also maintain the FBIHQ approval/denial response EC in the CHS Delta payment sub-file.

(U//FOUO) The FO may not make any additional payments to the CHS until the FBIHQ operational unit has advised that authority has been granted for continued payment.

(U//FOUO) The approval or denial communication will be signed by the authority level appropriate for the amount of the request, as follows:

- (U) Authority to exceed the $100,000 threshold and pay up to $200,000 requires operational DAD approval, which may be delegated down to the SC level.
- (U) Authority to pay a CHS more than $200,000 and up to $300,000 requires operational AD approval.
- (U) Authority to pay a CHS more than $300,000 and up to $400,000 requires operational AD approval.

- (U) Authority to pay a CHS more than $400,000 and up to $500,000 requires operational branch EAD approval.
- (U) Authority to exceed $500,000, and each $100,000 increment above $500,000, requires DD approval.

(U//FOUO) Delegated authorities within the FBIHQ operational divisions must be documented in advance to the appropriate operational division sub-file of [redacted] as directed in DIOG subsection 3.4.3.3.2.

### 17.5. (U) CHS Payment Categories: Services and Expenses

(U//FOUO) Requests for CHS payments must distinguish between payments for services and payments for expenses. Although records of both types of payments must be turned over to the FPO attorney, as appropriate (see as reference [redacted]), it is critical that each payment be accurately characterized in Delta and the FBI's financial system.

(U//FOUO) A CHS obtaining intelligence from a sub-source may be paid for reasonable services and/or expenses associated with that intelligence. The CHS, at his or her discretion, may in turn pay the sub-source from those funds. However, a CA or co-CA is not permitted to submit a draft request to compensate or reimburse a sub-source through the CHS.

#### 17.5.1. (U) Services

(U//FOUO) Service payments are those made to compensate a CHS for the information or assistance he or she provided to the FBI. The payments must be commensurate with the value of the information or assistance the CHS provided to the FBI, and must only be made after the services are rendered.

(U//FOUO) Service payments may be considered taxable income that must be reported to appropriate tax authorities. If a CHS is audited and requests payment documentation from the FBI to provide to the IRS, the FO may provide the CHS with a payment report that does not disclose the nature of the CHS's relationship with the FBI. For additional guidance, contact the HOS.

#### 17.5.2. (U) Expenses

(U//FOUO) Expense payments are those made to reimburse the CHS for reasonable costs incurred in direct support of an authorized FBI investigation or intelligence matter and for which the FBI and/or the USG derives the primary benefit.

(U//FOUO) Only payments made by a CHS to legitimate and lawful vendors are considered CHS expenses. Payments that a CHS makes to illegitimate or unlawful businesses (e.g., subjects, unwitting persons, illegal laborers) are considered case expenses, not CHS expenses. Likewise, all payments for the purchase of contraband or any other items of evidence are considered case expenses, not CHS expenses.

(U//FOUO) The FBI's reimbursement of CHS expenses must be based on the actual expenses incurred, with the exception of relocation expenses, which may be based on an estimate of the expenses (see subsection 17.6.6., "Relocation"). Original vendor receipts, or copies of vendor receipts, must be obtained in order to reimburse the CHS or, if an advance of funds is obtained, to reconcile the advance. If a receipt is lost or missing, the CHS must attempt to obtain a copy. In circumstances where obtaining a copy of a receipt is not feasible, the CA must prepare a

certification documenting the reason for the absence of a receipt (see subsection 17.7.2., "Vendor Receipts"). Once the actual expenses are ascertained, the CA must ensure that the amount reimbursed to the CHS is reasonable based on the relation of the expenditure to the FBI matter it supports.

(U//FOUO) If, due to exigent circumstances and with prior oral SSA approval, the CA must use personal funds to pay a CHS, or use a personal credit card or funds to purchase an item of value for a CHS (e.g., a purchase of a nonattributable telephone with personal funds) prior to submitting the payment or reimbursement request through the [redacted] payment process, the oral authorization must be documented in the CHS's payment sub-file as soon as practicable, but no more than five business days from date of oral approval. The CA must seek reimbursement in accordance with subsection 17.7.1., "Payment Request Entries," and subsection 17.6.5., "Equipment," if relevant. Under no circumstances may the use of personal funds, whether in an exigent circumstance or otherwise, exceed $1,000. Since this provision should only be used rarely, the authorizing SSA must ensure that the CA is exercising reasonable planning with the CHS whenever such a request is made.

(U//FOUO) Note that the purchase of equipment—such as a nonattributable telephone for use by the CHS's CA or co-CA to communicate primarily or exclusively with a CHS—must be done in accordance with [redacted] subsection 3.3.), and paid using case-related operational spending authority—not the CHS payment authority.

## 17.6. (U) Rules Regarding Expenses for Meals, Vehicles, Medical Costs, Housing, Equipment, and Relocation

(U//FOUO) The expenses addressed in this subsection may be covered as CHS expenses under the circumstances outlined below. Expenditures must be closely monitored to ensure that the government obtains the primary benefit from them, and it is the responsibility of the employee submitting a request for payment and the supervisor approving it to ensure that the expense is reasonable.

### 17.6.1. (U) Meals Associated With CHS Debriefings

(U//FOUO) Meal expenses incurred by a CA during a CHS debrief must be justified as an operational need. The full amount of the CHS's meal may be covered as a CHS expense, to the extent that the amount is reasonable and justified, based on the circumstances of the meeting. Government per diem rates may be used as a guide for reasonableness but are not determinative. Expenses attributable to the CA's meal, if justified, are covered by operational case funds. These expenses must adhere to government per diem rates. If they exceed those amounts, the CA must provide justification and obtain ASAC approval.

### 17.6.2. (U) Vehicles

#### 17.6.2.1. (U//FOUO) Government Vehicles

(U//FOUO) CHSs are prohibited from operating FBI vehicles. This includes Bureau vehicles assigned to FBI employees and vehicles obtained as a result of forfeitures. In addition, FBI personnel are prohibited from leasing or purchasing vehicles on behalf of CHSs. The parameters for supporting a CHS vehicle expense are set forth below.

#### 17.6.2.2. (U) Vehicle Maintenance

(U//FOUO) If a CHS uses his or her vehicle in support of an FBI investigation, the FBI may reimburse the CHS for basic maintenance expenses (e.g., oil changes, tire rotation/replacement) in an amount reasonably proportionate to the vehicle's use in furtherance of the FBI investigation. Requests for maintenance reimbursements must be supported by vendor receipts. If it is not possible to attach the original vendor receipt to the draft request because it reflects the CHS's true name, a redacted copy may be provided to the draft office. The true-name copy must be maintained in the CHS's main file (see subsection 17.7.2., "Vendor Receipts"). The redacted copy must then be scanned into the CHS's CE sub-file.

#### 17.6.2.3. (U) Vehicle Rentals

(U//FOUO) If it becomes necessary for a CHS to use a rental vehicle in furtherance of an FBI matter, the CHS must rent the vehicle in his or her name and provide the vendor receipt to the CA. The FBI may reimburse the expense in an amount reasonably proportionate to the vehicle's use in furtherance of the FBI investigation. an advance of funds may be given to the CHS in accordance with subsection 17.8.3., "Advance Expense Payments," if he or she does not have funds for the rental. After the rental receipt is provided to the FBI, the advance must be reconciled with the draft office.

#### 17.6.2.4. (U) Vehicle Purchases

(U//FOUO) On rare occasions, with prior approval from the responsible DI DAD, the purchase of a vehicle that will be used primarily in support of an FBI investigation may be a reimbursable a CHS expense. The CA must submit a request that includes:

- (U//FOUO) A statement that the vehicle will be used primarily in support of an FBI investigation.
- (U//FOUO) Facts demonstrating compelling operational need for the vehicle, including why the CHS is unable to use his or her own vehicle, rent or lease a vehicle, or use other modes of transportation.
- (U//FOUO) An explanation of the cost effectiveness of the purchase.
- (U//FOUO) A statement that the CA has determined that the CHS has a valid driver's license.

(U//FOUO) At the FO level, the request must be reviewed by the CDC and approved by the SAC. The request must then be forwarded to the appropriate [redacted] unit, which will coordinate legal review with OGC and approval from the appropriate operational unit.

(U//FOUO) The [redacted] must advise the CA of the final decision on the request. If the request is approved, the CHS must purchase the vehicle in his or her own name. If the CHS uses his or her own funds to make the purchase, the FO may reimburse the CHS through CHS funds as a CHS expense. If the CHS does not have sufficient funds to make the purchase, the CA may obtain an advance of funds to be given to the CHS in accordance with subsection 17.8.3., "Advance Expense Payments." The CHS must provide the purchase receipt to the CA, who must then reconcile the advance with the draft office.

(U//FOUO) At the conclusion of the investigation, the vehicle remains the property of the CHS. The FBI may not recover the vehicle from the CHS or assume responsibility for its disposal.

even if requested to do so by the CHS. The fact that the vehicle will remain the property of the CHS should be discussed with the individual prior to purchase. The value of the vehicle at that time is considered a service payment to the CHS. The individual must sign a CHS receipt for this value in accordance with subsection 17.7., "Payment Requests." The draft office must modify the original transaction in the FBI's financial system and the CA must modify the original FD-794b, "Payment Request," in Delta to reflect the value as a service payment.

### 17.6.3. (U) Medical Costs

(U//FOUO) If a CHS is injured as a direct result of his or her cooperation with the FBI (e.g., injured by subjects), the individual's medical costs may be covered as a CHS expense. This may be accomplished by obtaining [redacted] approval for CHS reimbursement for expenses incurred or, if the CHS does not have funds to cover the medical expenses, by obtaining [redacted] approval for an advance of funds in accordance with subsection 17.8.3., "Advance Expense Payments." The request must document the total medical costs and the circumstances under which they were incurred, it must be approved by the SAC and sent to the appropriate [redacted] unit, with copies of vendor receipts or invoices redacted as necessary to protect the identity of the CHS. The [redacted] must review the request, coordinate with the OGC and the appropriate operational unit at FBIHQ, and advise the FO of the decision via EC. If the request is not approved, the [redacted] must provide the basis for withholding approval. The request with supporting documentation and the decision to approve or deny the request must be filed in the CHS's payment sub-file.

(U//FOUO) If reimbursement is approved, the FO may reimburse the CHS through CHS funds as a CHS expense. If an advance of funds is approved, the CHS must provide documentation of the medical costs to the CA, who must then reconcile the advance with the draft office. In either instance, if the receipt contains the CHS's true name, a redacted copy must be provided to the draft office with the [redacted] and the original bearing the CHS's true name must be filed in the CHS's main file. Receipts must be provided for medical expenses (see subsection 17.7.2., "Vendor Receipts"). The redacted copy must then be scanned into the CHS's CE sub-file.

(U//FOUO) Generally, treatment for the CHS's preexisting medical conditions (e.g., allergies, infections, ulcers, heart attacks, mental conditions, dental work, or drug or alcohol addictions) that manifest after the CHS has been opened is not reimbursable as a CHS expense because it is difficult to discern whether the condition was incurred or exacerbated as a result of the CHS's cooperation with the FBI. Therefore, the CHS must utilize his or her own income (which would include any properly authorized service payments from the FBI) to cover these costs. However, the FO may request coverage of such expenses if justification can be provided that it is in the FBI's best interest to cover the medical costs in furtherance of an FBI matter and that the CHS's cooperation with the FBI caused or exacerbated the medical condition. The request must detail the medical conditions, costs, explanation of the way in which the CHS's cooperation with the FBI caused or exacerbated the medical condition, and the operational necessity of covering the expense. The request must be approved by the SAC and sent to the appropriate [redacted] unit, where the request will be processed in the same manner set forth above for medical expenses directly resulting from the CHS's assistance. The request and supporting documentation and the decision to approve or deny the request must be filed in the CHS's payment sub-file.

(U//FOUO) If a CHS is tasked to incur medical costs in support of a substantive investigation (e.g., as part of a healthcare fraud investigation), those costs should be designated not as CHS medical expenses, but as case expenses.

### 17.6.4. (U) Housing

#### 17.6.4.1. (U) CHS's Current Residence

(U//FOUO) If a CHS's personal residence is used to further an FBI matter (e.g., it is wired and monitored for daily meetings with subjects), the CHS may be reimbursed—based on vendor receipts and/or lease or mortgage agreements—for utility costs and monthly mortgage or rental payments as CHS expenses, in an amount reasonably proportionate to the use in furtherance of the FBI investigation. If it is not possible to attach a vendor receipt to the [redacted] because it reflects the CHS's true name, a redacted copy may be provided to the draft office and the true-name copy must be filed in the CHS's main file. Receipts must be provided for this expense (see subsection 17.7.2., "Vendor Receipts"). The redacted copy must then be scanned into the CHS's CE sub-file.

#### 17.6.4.2. (U) Temporary Housing

(U//FOUO) If a CHS does not live within a reasonable commuting distance to participate in an FBI investigation or, for the purposes of the case, needs to reside in a specific location, the CHS may be reimbursed for expenses related to a second place of residence. The FBI may pay reasonable expenses (e.g., hotel, rent, meals portion of the per diem rate) to maintain the CHS's temporary living quarters. The CHS must obtain the temporary housing and accept all liabilities associated with the temporary residence. FBI personnel are prohibited from entering into contractual renting or leasing of housing on behalf of a CHS, unless this is done in accordance with the [redacted] Another justification is when the temporary housing will support a Group I UCO in which an undercover business has been established. In this situation, the temporary housing may be obtained by the FBI through the undercover business, and the temporary housing costs covered by substantive case funding.

(U//FOUO) The FBI may continue to reimburse the CHS for the temporary housing as long as operationally necessary; however, ASAC approval is required every six months. The CHS must provide the original vendor receipt or lease agreement for reimbursement. If it is not possible to attach the original hotel or rent receipt to the [redacted] because it reflects the CHS's true name, a redacted copy may be provided to the draft office, and the true-name copy must be filed in the CHS's main file. Receipts must be provided for this expense (see subsection 17.7.2., "Vendor Receipts"). The redacted copy must then be scanned into the CHS's CE sub-file.

(U//FOUO) While residing in temporary housing, the CHS must pay any expenses associated with his or her permanent residence. These costs are not reimbursable CHS expenses.

### 17.6.5. (U) Equipment

(U//FOUO) The purchase of equipment (e.g., a cell phone, a computer, or a camera) may be covered as a CHS expense if the equipment will be used in support of an FBI investigation or assessment. The FO may reimburse the CHS through CHS funds as a CHS expense or, if an advance was paid, reconcile the advance with the draft office. The original vendor receipt for the equipment is required (see subsection 17.7.2., "Vendor Receipts"). If it is not possible to attach the original vendor receipt to the draft request because it reflects the CHS's true name, a redacted copy must be provided to the draft office, and the true-name copy must be filed in the CHS's main file. The redacted copy must then be scanned into the CHS's CE sub-file.

(U//FOUO) At the conclusion of the investigation, the equipment will remain the property of the CHS. The FBI may not recover the equipment from the CHS or assume responsibility for its disposal. The remaining value of the equipment is considered a service payment. The CHS must sign a CHS receipt for the remaining value and provide approximate resale value and documentation thereof to support the expense. This documentation must be uploaded into the CHS's CE sub-file in Delta. The draft office must modify the original transaction in the FBI's financial system, and the CA must update the original [redacted] in Delta to reflect the value as a service payment.

17.6.6. [redacted]

[redacted]

17.6.6.1. (U) Temporary Relocation

(U//FOUO) A temporary relocation for a short-term threat must be supported by a documented threat assessment that identifies the scope of the threat (e.g., until all the subjects are arrested or until the trial commences or concludes) and the danger area. Based on the details of the threat assessment and after the WSP threat and risk assessment has been submitted to [redacted] the SAC must determine a safe area where the CHS can temporarily relocate until the danger passes.

(U//FOUO) Government per diem rates should be used when determining expenses for lodging, meals, and incidentals. With SAC approval, the CA may reimburse the CHS through CHS funds as a CHS expense or provide the CHS an advance if the individual does not have funds to cover the approved relocation costs. The advance must be reconciled with the draft office and in Delta.

(U//FOUO) Liability and additional costs associated with the move and new location are the responsibility of the CHS. A hold-harmless agreement or clause stating this responsibility must be added to the CHS receipt (see subsection 17.6.6.2., below).

### 17.6.6.2. (U) Permanent Relocation

(U//FOUO) An FO's request for a CHS permanent relocation payment may include no more than 90 days of expenses for the CHS and/or his or her immediate family. These expenses may be calculated in one of two ways: by using either estimates or government per diem rates.

(U//FOUO) To use the estimate method, the CA must obtain at least three estimates for moving household goods, if necessary, and housing. Relocation payments may include the move of household goods by a moving company, travel (based on airline ticket price or government mileage rate) to the new location, rent (including the rental deposit, if applicable), meals portion of the per diem rate for the new area (compensation rates for children ten years of age and under should be half of the M&IE portion of the per diem), and utility costs (including the hook-up fee, if applicable) for up to 90 days. All requests and approvals, as well as all estimates and costs obtained by the CA, must be documented and maintained in the CHS's main file for auditing purposes. The average of the estimates/costs should be the dollar amount requested for the CHS and/or his or her immediate family's permanent relocation and should be classified as a CHS relocation expense on the [redacted]

(U//FOUO) Government per diem rates may be used in lieu of obtaining estimates to determine the reasonable expenses for lodging and M&IE for permanent relocations. Payment requests must clearly document the per diem rate used to support the requested funding. Compensation rates for children ten years of age and under should be half of the M&IE portion of the per diem. Per diem lodging should not be calculated for individual family members unless they will be living separately.

(U//FOUO) Whichever method of calculation is used, vendor receipts are not required to support the payment request. The payment request must be approved by the SAC (authority may be delegated to the ASAC). Thereafter, based on extenuating circumstances (e.g., a unique occupation or insufficient language skills), one extension of up to 90 days may be approved by the SAC (authority may be delegated to the ASAC). Any extension thereafter requires the approval of the appropriate [redacted] unit.

(U//FOUO) Liability associated with the relocation from the danger area to the new area and any additional costs not identified above are the responsibility of the CHS and cannot be reimbursed through CHS funds. A hold-harmless agreement or clause (see the [redacted] for a sample document) must be added to the CHS receipt, stating that:

- (U//FOUO) The FBI has identified or verified a threat against the CHS.
- (U//FOUO) The FBI recommends that the CHS and/or his or her immediate family relocate to the safe area identified by the CA.
- (U//FOUO) The FBI bears no liability for the CHS's and/or his or her immediate family's welfare after the payment is made.
- (U//FOUO) The FBI will not provide any additional funds for this or future relocations.

(U//FOUO) If the WSP was offered to the CHS and/or his or her immediate family and was refused, the CHS receipt must also note the refusal.

(U//FOUO) The CHS must initial the above advisements prior to receiving any funding from the FBI. Because this payment is based solely on the assessment conducted by the CA, the CHS does not have to document or explain how the payment was utilized. However, if it is know that the CHS failed to relocate, this fact must be documented in the CHS main file.

## 17.7. (U) Payment Requests

### 17.7.1. (U) Payment Request Entries

(U//FOUO) Service and expense payments to a CHS are requested by submitting an FD-794b ("Payment Request") in Delta, which must include:

- (U//FOUO) The substantive (i.e., operational) case title(s) and file number(s) for which the CHS provided the information.
- (U//FOUO) The date the CHS file was opened and/or reopened.
- (U//FOUO) The total amount previously paid to the CHS during the current FY.
- (U//FOUO) The total payment history (i.e., aggregate total), including the total amount previously paid to the CHS by any FBI FO. If the CHS was reopened, the [redacted] must include the total amount of payments previously made to the CHS.
- (U//FOUO) The total amount of the payment request. Payment requests for services and expenses may be included on the same [redacted] although the amount for each must be specified. If a CHS is to be paid for providing information for multiple investigative programs, the CA must specify payment amounts requested for each program on the [redacted] (e.g., "Cyber services – $500; Counterintelligence services – $1,000; Criminal expenses – $100"). The CA must include the investigative program file number and specific justification supporting the request.
- (U//FOUO) A detailed justification statement for the requested payment (see below). The specific justification for a service payment should be documented in detail and unique for the time period covered by the request. This provision applies to a CHS who is under a service agreement with the FBI.
- (U//FOUO) The payment method used. Cash or cashier's checks are the most common payment methods. If a method other than cash is used (e.g., a money order, a gift card, a non-reloadable debit card, or a Western Union-type wire transfer), a detailed justification for using that method must be provided on the [redacted] For more information regarding requisites for wire transfers, see subsection 17.9., "Paying a CHS."

(U//FOUO) Standard justification paragraphs are not acceptable and should be rejected by the approving SSA and certifying SAC (authority may be delegated to the ASAC). An expense reimbursement requires a specific breakdown of expenses (e.g., "$45.25 – cell calls; $123.58 – meals; $32.50 – gas") and a justification for each expense. CA and CHS expense reimbursements must be clearly separated and justified on the [redacted]—for example, CA meals exceeding the per diem; the use of an undercover credit card for the payment of a CHS expense; and other situations documented in the [redacted] which require specific SAC or ASAC approval.

### 17.7.2. (U) Vendor Receipts

(U//FOUO) Except when a CHS is being permanently relocated (see subsection 17.6.6.2., "Permanent Relocation"), the CHS must obtain vendor receipts for expenses incurred in support of an FBI matter. Prior to tasking the CHS to incur an operational expense, the CA must discuss with the CHS the requirement to obtain vendor receipts. The CA must note the CHS's S number on each vendor receipt and submit the receipts to the draft office with the [redacted] "Payment Request," in order to obtain a reimbursement or to liquidate an advance. Vendor receipts must be scanned into the CHS's CE sub-file to support the [redacted]

(U//FOUO) If the CHS cannot provide an original vendor receipt, a copy will be sufficient.

(U//FOUO) If a vendor receipt cannot be attached to the draft request because it reflects the CHS's true name, the CA must attach a copy of the receipt to the draft request with the CHS's name redacted. [redacted] The redacted copy must then be scanned into the CHS's CE sub-file.

(U//FOUO) In situations where requesting a receipt from the vendor would endanger the CHS or disclose the CHS's relationship with the FBI, and in rare instances where the receipt is lost, the CHS must advise the CA of the amount spent and the reason for not providing a vendor receipt. The CA must submit a certification with the [redacted] for the expense. The certification must contain the following: 1) a statement that the CHS advised the CA of the amount spent; 2) the date the CA received notification; 3) the circumstances that precluded the CHS from obtaining or caused the CHS to lose the receipt; and 4) the reasonableness of the expense.

## 17.8. (U) Payment Approvals

### 17.8.1. (U) FPO Attorney Approval

(U//FOUO) If an FPO attorney is participating in an investigation that is using a CHS who is expected to testify, the CA must obtain approval from the FPO attorney, in advance if possible, for payments made to the CHS. The FBI may obtain approval for a specific payment amount or a potential range of aggregate CHS payments that could be made for the duration of an investigation. If the CA proposes making payments for services and the FPO attorney objects, no service payment may be made until the dispute has been resolved through the AGG-CHS dispute resolution process. (See subsection 1.5.1., "AGG-CHS and AGG-Dom Exceptions and Dispute Resolution.")

### 17.8.2. (U) FBI Field Office Approval

(U//FOUO) CHS payment requests require SAC approval. The final approver of the [redacted] bears the responsibility of ensuring the accuracy of the payment request and compliance with all CHS policies, the [redacted] and other federal government regulations and policies (e.g., those on travel and procurement). The final approver, therefore, must sign as the "certifier," indicating his or her certification of compliance, before the [redacted] can be submitted to the draft office.

(U//FOUO) In limited situations where a payment must be made immediately due to operational or security reasons, and SAC approval cannot be obtained prior to the payment, the SAC must be notified of the payment within 24 hours. The CA must document the notification to the SAC in the CHS sub-CE within 24 hours.

### 17.8.3. (U) Advance Expense Payments

(U//FOUO) The SAC may approve expense payments to a CHS in advance of the expenses being incurred for up to $50,000 per payment, totaling no more than $100,000 per FY. The payment request must document the justification for the need to advance funding to the CHS. Approval of an advance is appropriate in situations where a CHS is expected to incur significant expenses in connection with his or her operation, such as operational travel. When funds are advanced, the CA must ensure that the actual expenses incurred by the CHS are supported with vendor receipts or, where allowed, CA certification (see subsection 17.7.2., "Vendor Receipts"). Based on the vendor receipts or certification, the actual expenses are to be reconciled with the advance of funds. After the CHS submits the vendor receipts and any unused funds, he or she must sign a second receipt that reflects the actual amount spent and any funds the CHS returned to the CA. The CA must ensure that the appropriate amount for the payment is reconciled in Delta and recorded in the sub-CE file.

## 17.9. (U) Paying a CHS

(U//FOUO) After obtaining the approvals outlined in subsection 17.7., "Payment Requests," and subsection 17.8., "Payment Approvals," the SA must submit the Delta draft version of the [redacted] to the draft office. The draft office will issue a draft check or deposit funds into the SA's government-issued account. The SA may withdraw funds from his or her debit card or cash the draft check to make the payment. If it is not operationally feasible to pay the CHS in cash, the SA may convert the funds to another form of payment, such as a cashier's check, money order, or non-reloadable debit card, after documenting the justification for the alternate form of payment in accordance with subsection 17.7.1., "Payment Request Entries."

(U//FOUO) The SA, with another SA or other government official, must witness the payment to the CHS. An SA may request that an FBI professional staff employee serve as a witness if, after a reasonable effort has been made, no other SA, LEO, or person in a comparable position can be located. The request must be in writing, provide justification for the use of the professional staff employee, and be approved by the SSA of the squad with oversight for the CHS and the professional staff employee's supervisor. This communication must be retained in the CHS's sub-CE file.

(U//FOUO) In the event of extraordinary circumstances that must be documented in the CHS's file and approved by the SAC, only one witness is required. The request must be in writing, provide justification for the witness waiver, and be maintained in the CHS's sub-CE along with the SAC's approval.

(U//FOUO) The CHS must sign and date a written receipt at the time of payment for each payment, using his or her assigned payment name. The signed payment receipt must contain the witnesses' signatures, the payment date, the period covered by the payment, and the amount paid for services vs. expenses. The receipt must be maintained in the CHS's sub-CE file.

(U//FOUO) If it becomes necessary to make a correction on the CHS receipt, the correction must be made in the presence of the CHS, and the CHS must initial the change. If an error is identified after the paying SA and witness depart from the CHS, the CHS must sign a new receipt, which must be witnessed in the same manner as if an original payment were being made. If the SA is unable to meet with the CHS (e.g., if the CHS moved out of the area and the SA does not have the CHS's contact information), the SA must initial the modifications to the CHS receipt and

document that he or she was unable to reach the CHS prior to submitting the CHS receipt to the draft office and scanning it into the CHS's sub-CE.

(U//FOUO) At the time of payment, the FBI agent or other government official must advise the CHS that the monies may be taxable income that must be reported to appropriate tax authorities. An SA must not provide tax advice to the CHS, but should instruct the CHS to contact a tax consultant of the CHS's choice for tax advice if he or she has any questions. The advisement that the payment may be taxable income must be documented in the sub-CE file.

(U//FOUO) The SA must make reasonable efforts to ensure that the CHS is paid in person. This includes traveling to meet the CHS or transferring the funds to another FO or Legat with a request that an SA in that office and another SA or government official make and witness the payment.

(U//FOUO) If, for operational or security reasons, payment cannot be made in person, the SAC may approve payment via a wire transfer (or other electronic means) or by loading or reloading an electronic stored value card, such as a prepaid credit or debit card. The transfer of funds from the remote location must be witnessed by an SA and another SA or government official and documented in the CHS file. The CHS must provide the SA with same-day written acknowledgment of receipt of the payment. The written acknowledgement must include the date and signature of the CHS.[7] In order to satisfy the requirement for a signature, the CHS must use his or her assigned payment name. In rare circumstances, the CHS may use a preapproved pseudonym for the payment receipt acknowledgement if operational security concerns are raised regarding the use of the CHS payment name. The prior SSA approval for the use of the pseudonym and the basis for its use must be documented in the CHS main file. If the CHS sends the payment receipt acknowledgement via e-mail, the e-mail must be sent to an account not attributable to the USG.

(U//FOUO) A wire transfer to a bank account associated with the CHS requires prior approval from the SAC, the appropriate [redacted] unit, and the FD and must be documented to the CHS sub-CE file.

### 17.10. (U) SSA Financial Audit of Payments

(U//FOUO) In preparing the QSSR for a review period in which a CHS has been paid, the SSA must ensure that the following requirements have been documented in the CHS file:

- (U//FOUO) The payment request specifies the amount of money attributed to each program (Criminal, Cyber, Counterterrorism, or Counterintelligence) supported by the CHS.
- (U//FOUO) Approval for the payment to the CHS is documented on an [redacted]
- (U//FOUO) The payment receipt was signed by an FBI SA and another SA or other government official, unless a waiver was granted (see subsection 17.9., "Paying a CHS.")
- (U//FOUO) The receipt was signed and dated by the CHS at the time of payment.

---

[7] A typed name constitutes a signature in this circumstance.

- (U//FOUO) The period covered is indicated on the receipt and matches the [redacted]
- (U//FOUO) The receipt appropriately distinguishes whether the payment is for services or expenses.
- (U//FOUO) The CHS initialed the tax advisement for all service payments.
- (U//FOUO) All CHS payments are documented in the CHS's CE sub-file and reconciled.
- (U//FOUO) Annual and aggregate payment authorities have not been exceeded.

## 17.11. (U) Acceptable Uses for Service Agreements

(U//FOUO) A service agreement is a binding contract between the FBI and the CHS; therefore, there is a need for consistency in language across the FBI. Accordingly, all service agreements must be drafted using the language provided in the service agreement form (see Appendix F, "Service Agreement"). The "Mandatory" language must be used, as written, in every service agreement, and the "If Applicable" language must be used, as written, in situations where it is appropriate. Any omission of mandatory language, modification of the "Mandatory" or "If Applicable" language, or addition of language not provided requires OGC approval, which the [redacted] will coordinate. OGC approval of language modification must be sought prior to presenting the agreement to the CHS for signature. OGC/CDC review is not required if the service agreement is drafted in accordance with the preapproved language. If no modifications of the provided language have been made, see the following paragraph for the approval process.

(U//FOUO) All CHS service agreements must be approved by the SAC and then by the appropriate DI SC, the FD, and the operational division SC, as coordinated by the [redacted] before being presented to the CHS for signature. The CA must prepare an EC containing justification for the agreement and route that communication, with the draft service agreement, for SAC approval. If applicable, coordination with the FPO participating in the conduct of an investigation or prosecution that is utilizing the CHS is required prior to SAC approval. If approved, the package (i.e., the draft service agreement and SAC approval) must then be submitted to the appropriate [redacted] unit via e-mail. The [redacted] unit must review and coordinate the approval of the agreement through the appropriate operational unit, the FD, and the SC, DI. The approved agreements will be forwarded by the [redacted] unit to the FO contracting officer's representative (COR) (which must be the CA, co-CA or another SA) identified in the agreement.

(U//FOUO) Upon receipt of the FBIHQ-approved and signed agreement, the COR (i.e., the CA, co-CA, or another SA, in the presence of another agent or government official as a witness) must present the agreement to the CHS for signature in payment name and subsequently provide the signed agreement to his or her FO CHSC to be scanned into the CHS's main file. The hard copy must be retained in the CFR. If the signed agreement is routed or otherwise internally disseminated outside the CFR, the payment name of the CHS must be on that copy.

(U//FOUO) In order to pay the CHS under the agreement, the [redacted] must include the signed agreement that clearly documents the information and/or assistance provided which warrants the dollar amount identified in the agreement. The CHS cannot be paid more or less than the contracted amount by the FO or any other FO utilizing the CHS. If a CHS does not provide the information/assistance that warrants the dollar amount, the agreement must be terminated or modified in accordance with subsection 17.11.1., "Modification, Expiration, Renewal, and Termination of Service Agreements."

(U//FOUO) The SAC must review all CHS service agreements every six months to determine whether the agreement may continue for another six months. Review criteria must include whether an operational need for the agreement still exists and, if service payments are included, whether the amount listed is commensurate with the services being provided. The SAC review must be acknowledged in writing and placed into the CHS main file. All agreements terminate within 12 months of the CHS's signature on the agreement, unless extended in accordance with subsection 17.11.1., below.

(U//FOUO) A service agreement is between the CHS and the FBI, not between the CHS and an FO. Therefore, any FO utilizing a CHS under contract must abide by the terms of the service agreement. The SAC is responsible for ensuring compliance with the terms of the agreement and the termination of the agreement.

(U//FOUO) Approval of service agreements does not provide an enhancement of annual or aggregate payment authorities. These authorities must be requested separately, as noted above in subsection 17.3., "SAC Annual CHS Payment Authority," and subsection 17.4., "Aggregate Payment Authority."

(U//FOUO) CAs must consider that a service agreement may preclude the CHS from receiving a lump-sum payment at the conclusion of the investigation and will reduce any request for a forfeiture award. The information and assistance provided during the time period for which a CHS is under an agreement cannot be utilized as justification for either a lump-sum or forfeiture award.

### 17.11.1. (U) Modification, Expiration, Renewal, and Termination of Service Agreements

(U//FOUO) An FO is prohibited from making modifications to an agreement after it has been approved at FBIHQ. However, a modification request may be submitted using the same process required for initial approvals.

(U//FOUO) A service agreement expires 12 months from the date of acceptance (i.e., the date of the CHS's signature). If the FO deems it feasible to continue the agreement, it must submit a renewal request using the same process required for initial approvals.

(U//FOUO) If an FO decides to terminate an agreement prior to its expiration, and a payment is due to the CHS under the agreement, the termination must be documented and initialed on the CHS receipt for the last service payment under the terms of the agreement. If the CHS is not due to be paid under the agreement, the agreement must be terminated via a letter signed by the SAC, with a copy sent to the CHS payment sub-file.

(U//FOUO) If the CHS decides to terminate the agreement, the CHS must provide written notice. This requirement must be included in the agreement. Documentation noting the CHS's termination must be placed in the CHS payment sub-file.

## 17.12. (U) Payments to CHSs by Other Field Offices

(U//FOUO) To ensure that annual or aggregate payments do not exceed the payment authorities (see subsection 17.2., "Field Office Funding for CHSs," subsection 17.3., "SAC Annual CHS Payment Authority," and subsection 17.4., "Aggregate Payment Authority"), all payments to a CHS made by another FO must be coordinated with the OO. Payments may be made by either the OO or the FO which utilized the CHS. The payment authority, however, always remains the

responsibility of the OO. All payments must be documented in the CHS's sub-CE file and be reconciled in Delta.

### 17.13. (U) Gifts in Lieu of Monetary Payments

(U//FOUO) An SAC may approve the purchase of a gift in lieu of a service payment in limited circumstances, such as when there are facts to indicate that a CHS whose assistance justifies a service payment will not accept a cash payment. Prior to submitting a request to purchase a gift, the CA must ensure that the CHS is willing to accept a gift of appreciation from the FBI. SAC approval must be granted before the gift may be purchased. Plaques, mementos, and similar items may not be presented to CHSs who are incarcerated or who have extensive criminal histories. An FO must not use CHS funding to purchase gifts for the CHS in recognition of a notable occasion (e.g., a birth, an illness, a marriage, or a graduation) or for the CHS's family members or friends.

(U//FOUO) The value of the gift must be documented by a vendor receipt in order for the CA to be reimbursed or obtain an advance.

(U//FOUO) Because the gift is a service payment, a written payment receipt must still be executed in accordance with subsection 17.9., "Paying a CHS."

### 17.14. (U) Lump-Sum Payments

(U//FOUO) A CA may request a lump-sum payment for a CHS at the conclusion of any investigation in which the CHS has made significant contributions to FBI investigative matters or at the conclusion of the CHS's operation for the FBI. The CHS may only receive a lump-sum payment for information or assistance for which he or she was not previously compensated. This does not preclude a CHS from receiving a lump-sum payment for the same investigation for which he or she previously received service payments; however, the lump-sum payment must compensate the CHS for information or assistance not previously compensated.

(U//FOUO) Each lump-sum payment request must address the significance of the investigation and the CHS's contributions to it. The following information must be included in any request for a lump-sum payment:

- (U//FOUO) Title and file number of the case to which the CHS contributed information
- (U//FOUO) Details regarding the significance of the investigation
- (U//FOUO) Justification for the lump-sum payment (must be for assistance not previously compensated)
- (U//FOUO) Statistical accomplishments attributed to the CHS's information or assistance that support the lump-sum payment
- (U//FOUO) Whether the CHS suffered any financial loss (not previously compensated) as a result of his or her cooperation in the investigation
- (U//FOUO) The total amount of services and total amount of expenses paid to the CHS for the FY and in the investigation, and the total service payments paid to the CHS for the investigation(s) described in the first point above
- (U//FOUO) Whether the assigned FPO concurs with the payment (if the CHS is to testify or has testified)

- (U//FOUO) The value of seized or forfeited property obtained as a result of the CHS's cooperation and whether the CHS has received or would be nominated for an award or nominated for a payment resulting from forfeited assets
- (U//FOUO) Whether the CHS has or will receive any payment for services or expenses from any other LE agency(ies) in connection with the information or services that he or she provided to the FBI

(U//FOUO) The lump-sum payment request must be approved by the SAC. A lump-sum payment must be paid from the FO's budget, subject to the SAC's annual payment authority. If the payment is within the SAC's payment authority, but the FO's budget has insufficient funding, an enhancement request must be coordinated through the budget unit of the appropriate operational unit (see subsection 17.2., "Field Office Funding for CHSs").

(U//FOUO) A lump-sum payment request that exceeds the SAC's annual authority and/or one of the aggregate $100,000 incremental thresholds must be submitted to the appropriate operational unit for approval in accordance with subsection 17.3., "SAC Annual CHS Payment Authority." The operational unit is responsible for evaluating the amount of the requested lump-sum payment against the operational benefit provided by the CHS's assistance. Operational unit recommendations must be approved at the appropriate authority level within the respective divisions, as stated in the [redacted]. The operational unit must advise the FO and notify the appropriate [redacted] unit of the decision rendered on the request.

## 17.15. (U) Rewards

### 17.15.1. (U) Rewards Offered by Entities Outside the FBI

(U//FOUO) A CHS may accept rewards from another entity offered as a result of his or her assistance. The reward must be documented in the CHS's sub-CE file. Approval to disclose the CHS's identity may be necessary in accordance with Section 15, "Disclosure of a Confidential Human Source's Identity." If it is necessary for a CA or a co-CA to receive the reward on behalf of the CHS to protect the CHS's identity, the CA or co-CA must document the receipt of the reward and the transfer of the reward to the CHS. The CA's or co-CA's transfer of the reward to the CHS must be witnessed by the CA or co-CA and another SA or other government official, and the CHS must sign a receipt, as with any other payment, in accordance with subsection 17.9., "Paying a CHS."

### 17.15.2. (U) Rewards Offered by the FBI

(U//FOUO) The policy on acceptance of FBI publicly advertised rewards is detailed in [redacted]

## 17.16. (U) Forfeiture Awards

(U//FOUO) A CHS may receive an award based on a forfeiture even if he or she has already been compensated for the information and/or assistance that directly led to the forfeiture. However, the forfeiture award must be offset by any previous payments for information or assistance which led to the seizure, excluding expense payments.

(U//FOUO) A CHS may receive compensation of up to 25 percent of the net value of the forfeited property, not to exceed $500,000 per forfeited asset.

(U//FOUO) The forfeiture award request must be approved by the SAC and submitted to the HOS under the CHS S number. The EC must include:

- (U//FOUO) A copy of the final judicial order of forfeiture or declaration of administrative forfeiture.
- (U//FOUO) The name and opinion/concurrence of the FPO, AUSA involved in the operation of the CHS regarding payment to the CHS with forfeited proceeds, if applicable.
- (U//FOUO) The total value of the forfeited property.
- (U//FOUO) The amount of actual cash or residual proceeds, if known.
- (U//FOUO) The percentage of equitable sharing (the sharing disbursement is based on the remaining funds after all expenses have been deducted, including forfeiture awards).
- (U//FOUO) A detailed justification for the payment of an award, including the information or assistance provided by the CHS that directly resulted in the seizure/forfeiture of the property.
- (U//FOUO) Verification that the USMS has been notified of the FBI's intent to pay an award on the forfeited property. Forfeiture personnel in an FO are responsible for forwarding a communication to the USMS documenting the FBI's intent to pay an award based on the forfeiture, and checking the award block on the sharing forms [redacted] The notification must be documented in the CHS's main file.
- (U//FOUO) The total amount of services and total amount of expenses paid to the CHS for the FY in which the property was seized or forfeited, and a brief justification for all service payments.
- (U//FOUO) Verification that the CHS was not previously compensated for the information or assistance that led to the seizure/forfeiture of the property for which the award is being sought, if prior payments have been made for such information or assistance, the communication must identify such payments.

(U//FOUO) If the forfeited property will be placed into official use, the appraised value is used to determine the award. All other property must be sold and the proceeds deposited by the USMS prior to a determination of the award amount.

(U//FOUO) The CA or co-CA must submit the request for forfeiture awards to the appropriate operational unit upon receipt of the final judicial order of forfeiture or declaration of administrative forfeiture prior to any equitable sharing. The operational unit must evaluate the requested award payment against the operational benefit provided by the CHS and coordinate the approval of the request with the [redacted] FD.

(U//FOUO) The operational unit must prepare the approval communication for the FO, with notification to the appropriate [redacted] unit and [redacted] and coordinate the necessary transfer of funding.

### 17.17. (U) Project-Generated Income

(U//FOUO) An FBI operation involving a CHS may produce income. In order for the FBI to use that income, commonly called "project-generated income" (PGI), to offset the necessary and

reasonable expenses incurred by the operation, the appropriate [redacted] unit must obtain an Attorney General (AG) exemption.

(U//FOUO) [redacted] and operational unit authority may be granted for a CHS to be compensated for services and expenses with PGI, provided that all operational costs have been covered. Upon SAC approval and concurrence of the FPO attorney involved in the operation of the CHS (if applicable), the CA must submit a communication in accordance with the [redacted]

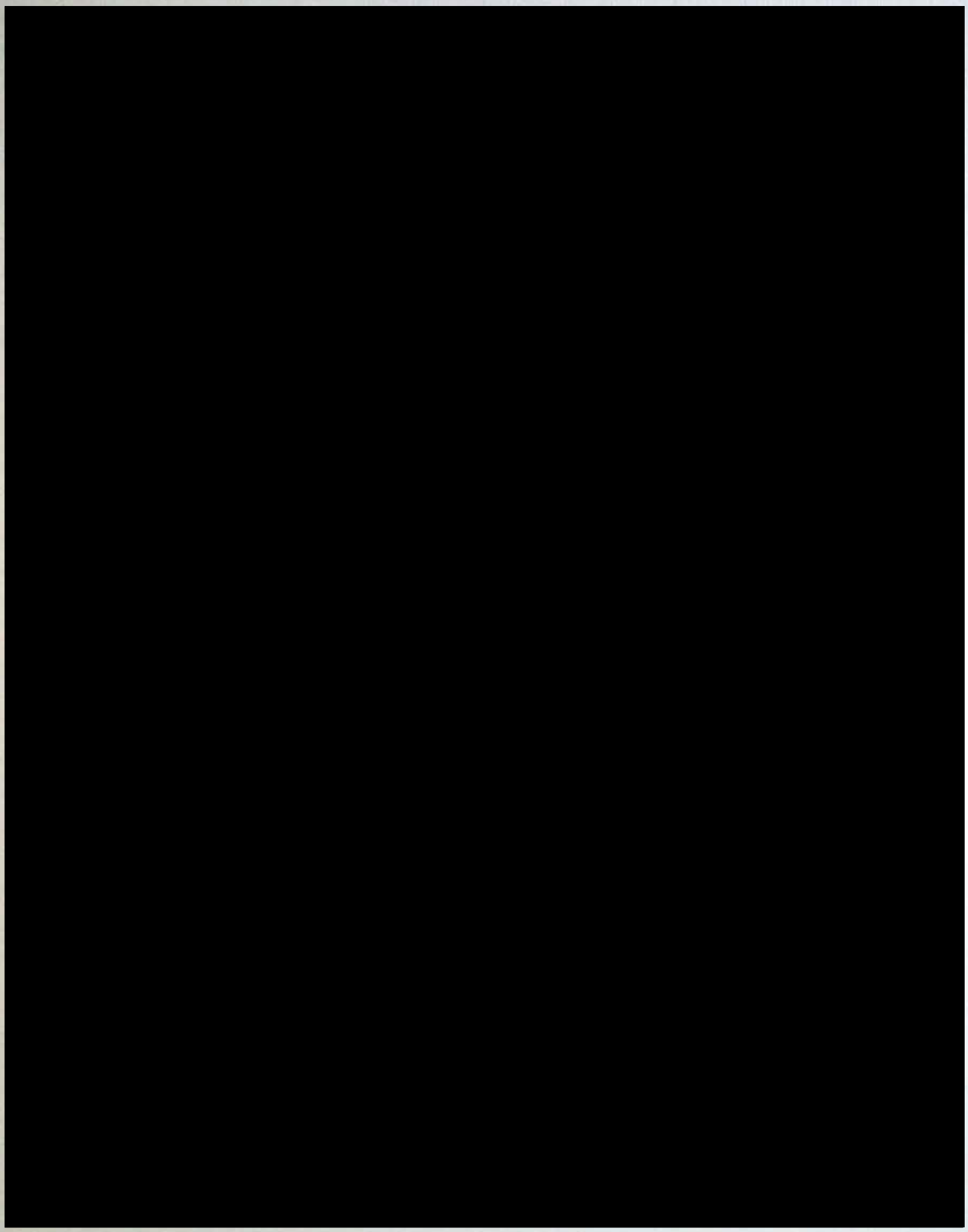
(U//FOUO A CHS may be paid from PGI funds or from CHS funds; however, PGI funds must not be commingled with CHS funds. Therefore, FOs must clearly document in the CHS's sub-CE the termination of PGI funding for CHS payments and the commencement of CHS funding. PGI payments must be documented in Delta.

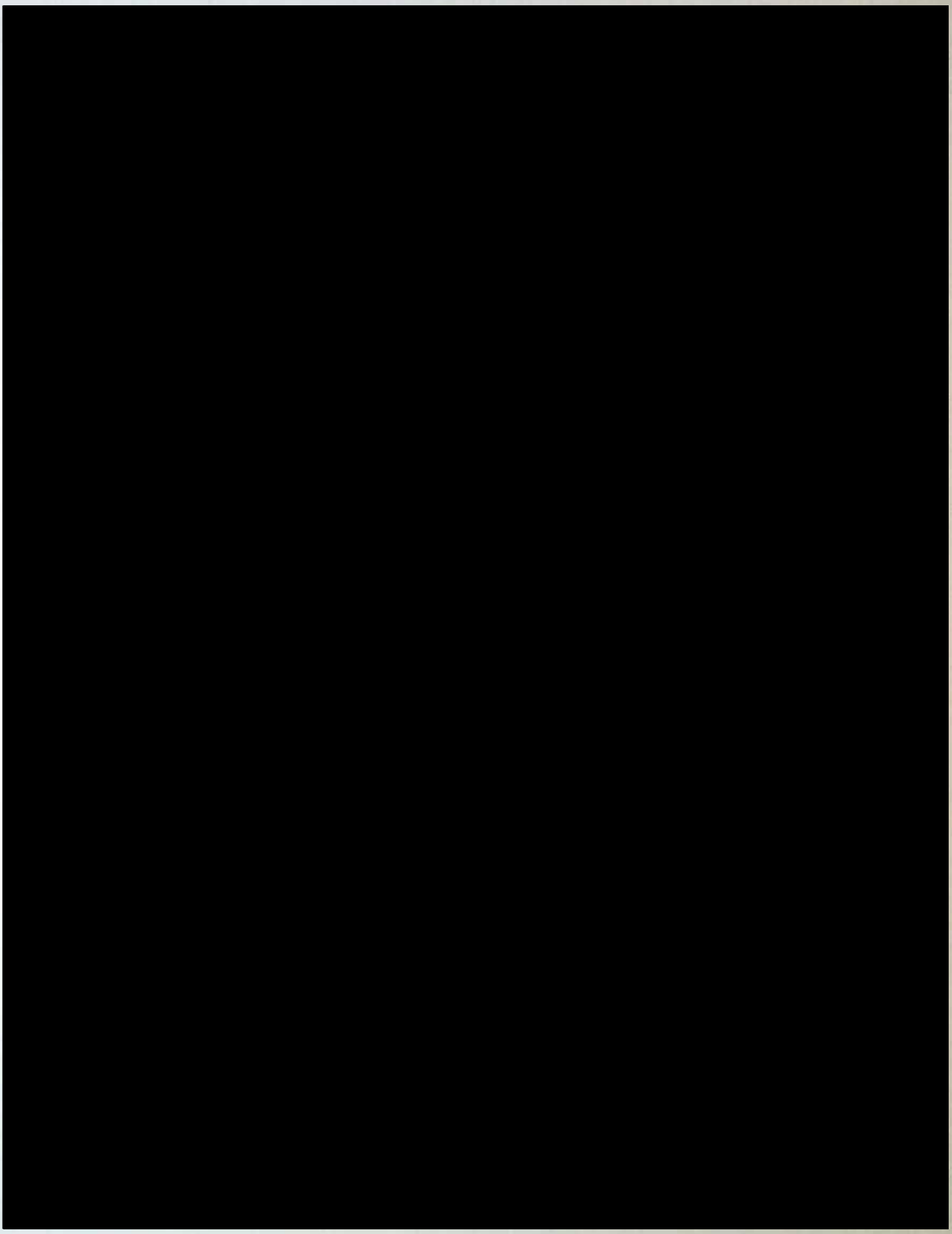
### 17.18. (U) Funds/Gifts Given to a CHS by a Subject

(U//FOUO) With the exception of funds paid for goods and services rendered in legitimate business transactions, any money, illegal proceeds (e.g., gambling, loan sharking, sale of contraband), or gifts received by a CHS from any individual or group that is a subject or potential subject of an FBI investigation must be turned over to the FBI. Disposition of such funds or gifts should be in accordance with the [redacted] and with subsection 2.3.1., "Gifts."

### 17.19. [redacted]

[redacted]





17.19.2. [redacted]

[redacted]

### 17.20. (U) Payments to a Closed CHS

(U//FOUO) Generally, a CHS may not be paid if he or she is in a closed status. In the rare event that a payment must be made either for services or expenses, the SAC may authorize a one-time payment to a CHS who has been closed. If more than one payment must be made to a CHS who has been closed, the CHS must first be reopened according to the requirements of subsection 4.5., "Requirements for Reopening a CHS."

### 17.21. (U) One-Time Non-CHS Payment

(U//FOUO) The limits and requirements described in this subsection apply to non-CHS payments. With SAC approval, only one payment may be made to any individual who has provided information to the FBI in furtherance of an FBI investigation, but who has never been opened as a CHS for the FBI. For payments in excess of $100,000, a communication requesting the amount desired, with a justification, must be submitted to [redacted] for approval. A non-CHS may only be paid for services rendered and/or expenses incurred by that individual, as defined above in subsection 17.5.1., "Services," and subsection 17.5.2., "Expenses." Payments to non-CHSs are charged to the CHS budget using the appropriate case file number.

(U//FOUO) Before approving a payment to a non-CHS, the SAC should weigh the benefits gained by making such a payment against the risks involved in not tracking the person as contributing to the FO's and the FBI's intelligence base and not providing protection to the individual's identity.

(U//FOUO) Non-CHS payments may not be used for the reimbursement of the expenses of agents or other LE or IC officials.

(U//FOUO) If payments are made to a non-CHS, the FO CHSC must open a file dedicated to tracking these payments in order to capture that person's contributions to the intelligence base and the amount of funds paid.

### 17.22. (U) Payments to a Non-CHS Requiring Maintenance and Security

(U//FOUO) CHS funds must not be used for the maintenance or security of an individual who has never been opened as an FBI CHS, but who requires maintenance and security because of his or her cooperation with the FBI. This includes individuals awaiting WSP entry. SAs are prohibited from opening these individuals as CHSs merely for payment purposes. SAs must use FO case funding or funding from the FPO for maintenance and security or relocation payments for these individuals. See Section 8., "Witness Security Program."

### 17.23 (U) CHS Providing Money or Property in Support of an FBI Investigation

(U//FOUO) In order for a CHS to provide money or property in support of an FBI investigation the ASAC must make a written finding that the acceptance of the CHS's money or property is necessary and appropriate for operational reasons. The written finding must include a determination whether the circumstances create the potential for coercion or an appearance of coercion of the CHS. This written finding must be documented in the validation sub-file.

# 18. (U) Closing a Confidential Human Source

## 18.1. (U) Closing Communication

(U//FOUO) When a determination has been made to close a CHS, a communication documenting the reason for closing must be included in the CHS's main file. Those reasons are listed below in subsections 18.1.1. and 18.1.2., below. Although more than one reason may exist for closing a CHS, if one of the reasons would justify closing the CHS for cause, the closed-for-cause category must be selected as the basis for closing.

### 18.1.1. (U) General Reasons for Closing a CHS

(U//FOUO) A CHS may be closed because:

- (U//FOUO) Confidentiality has been unintentionally compromised.
- (U//FOUO) The CHS's cooperation has been completed.
- (U//FOUO) The request to operate the CHS has been denied by FBIHQ or another agency.
- (U//FOUO) The CA transferred.
- (U//FOUO) The CHS:
  - (U//FOUO) Has died.
  - (U//FOUO) Has entered the WSP.
  - (U//FOUO) Is in poor health.
  - (U//FOUO) Has requested termination.
  - (U//FOUO) Has relocated, or is unavailable.
  - (U//FOUO) Has been unproductive.
  - (U//FOUO) Is no longer in a position to report.

### 18.1.2. (U) Closing a CHS for Cause

(U//FOUO) The decision to close a CHS for cause, as opposed to a general reason, must be based on a consideration of the seriousness of the facts and circumstances of each case. The decision to close for cause, however, is required if there is grievous action by the CHS or a discovery of previously unknown facts or circumstances that make the individual unsuitable for use as a CHS. Documenting that a CHS was closed for cause also establishes a record regarding the severity of the CHS's conduct that will guide other SAs who may consider reopening the CHS in future.

(U) The following is a list of reasons that might justify closing for cause:

- (U//FOUO) UIA
- (U//FOUO) Unreliability
- (U//FOUO) Unwillingness or inability to follow instructions
- (U//FOUO) Serious control problems

### 18.2. (U) Closing Procedure

(U//FOUO) Upon closing the CHS, whether for cause or for a general reason, the CA and one other FBI SA, LEO, or person with a comparable position in a U.S. intelligence agency serving as a witness, must:

- (U//FOUO) Advise the CHS, if the CHS can be located, that he or she is closed.
- (U//FOUO) Document that such notice was given and whether the CHS acknowledged receipt and understood.

(U//FOUO) If the CHS refuses to acknowledge these advisements, the refusal must be documented in the same manner, witnessed by the CA and the witness in one of the positions described above.

(U//FOUO) In addition, if the CHS was authorized to participate in OIA, any pending authorization must be revoked in accordance with subsection 13.8., "Revocation of OIA Authorization."

(U//FOUO) When a CHS is closed for cause, the CA must provide written notification of the closing communication to the ASAC (or via successor form in Delta), and a copy must be maintained in the CHS's validation sub-file.

(U//FOUO) When a CHS is closed for cause, subsequent contact with the individual requires special authorization (see subsection 18.3., "Future Contact With a Closed CHS"). In addition, a request to reopen a CHS who was closed for cause requires additional justification and supervisory scrutiny (see subsection 4.5.1., "Request to Reopen a CHS Previously Closed for Cause").

#### 18.2.1. (U) Delayed Notification

(U//FOUO) In the event that the CA or co-CA has determined that there is sufficient reason to close a CHS, but providing an immediate notification to the CHS would likely jeopardize an ongoing investigation or prosecution or cause a flight from prosecution, a decision may be made to delay the notification. The decision and supporting justification must be documented in the CHS's main file.

### 18.3. (U) Future Contact With a Closed CHS

(U) Absent exceptional circumstances that are approved (in advance, whenever possible) by an SSA, an agent must not initiate contact with or respond to contacts from a former CHS who has been closed for cause. Approval for such contact must be documented in the CHS's main file. CHSs who were closed, but not for cause, may be re-contacted without prior approval.

(U) New information may be documented to a closed CHS file; however, the CHS must be reopened if the relationship between the FBI and the CHS is expected to continue beyond the initial contact or debriefing.

(U) To make payments to a closed CHS, see subsection 17.20., "Payments to a Closed CHS."

### 18.4. (U) Coordination With FPO Attorneys

(U//FOUO) If an FPO attorney is participating in the conduct of an investigation that is utilizing an FBI CHS or the FPO is working with a CHS in connection with a prosecution, the CA must

coordinate (in advance, whenever possible) with the FPO attorney assigned to the matter regarding any decisions described in this section

## 19. (U) Extraterritorial[8] Operations

(U//FOUO) Unless specified otherwise in this section, all other provisions of this PG apply to ET CHS operations. All ET operational approval authority levels may be delegated one supervisory position level, unless specified otherwise. In addition, approval may be provided by a properly authorized individual in an acting capacity or by a person holding a more senior position than required by this PG.

(U//FOUO) This section provides standardized policy for all investigative program areas related to both ET CHS operational activity and nonoperational travel. Adherence to this policy for both CHS international operational and known nonoperational travel promotes effective coordination among affected parties and mitigates the risk inherent in such activities.

(U//FOUO) The following authorities, to the extent to which they apply to ET operations, govern the policy for ET CHS operations:

- (U) *The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection* (NSIG) (October 31, 2003)
- (U) *Attorney General Guidelines for the Development and Operation of FBI Criminal Informants and Cooperative Witnesses in Extraterritorial Jurisdictions* (January 7, 1993)
- [redacted]
- (U) "Memorandum of Understanding Concerning Overseas and Domestic Activities of the Central Intelligence Agency and the Federal Bureau of Investigation" (July 29, 2005) (hereafter referred to as the "FBI/CIA MOU")

(U//FOUO) The aforementioned authorities differentiate between CHS operations in support of national security and criminal investigations; thus, different policy requirements are mandated for each type of CHS operation. In addition, FBI policy differentiates between the aforementioned investigation types and positive foreign intelligence (PFI) operations. Therefore, this section establishes different approval levels and policy standards for a CHS operation in support of a national security investigation, a PFI investigation, and a criminal investigation. However, whenever permissible under the above authorities, FBI process and policy will be consistent for all CHS ET operations. When applicable, the heading of each subsection indicates whether it is applicable to national security, PFI, criminal, or all investigations. If an ET CHS operational request is in support of both a national security investigation and a criminal investigation, the policies and approvals for operation in support of a national security investigation apply.

(U//FOUO) Based upon the category of CHS activity, specific approvals, notifications, and documentation requirements apply. These categories are defined as follows:

[8] (U) "Extraterritorial" refers to any body of land or water beyond the territorial jurisdiction of the United States.

- (S//NF) **CHS ET operational travel**: The CHS travels to a foreign country from the United States[9] or from one foreign country to another foreign country to engage in operational activity (e.g., when tasked to collect intelligence or evidence) on behalf of the FBI. This activity may be declared or undeclared to the host country, and may be unilateral or a joint operation.
- (S//NF) **CHS ET resident**: The CHS resides in a foreign country.
- (S//NF) **CHS ET debrief**: In support of an FBI or a USIC objective, the CHS travels at the request of an FBI employee to meet in a foreign country for a debriefing, for training, or to receive passed items or be assessed. See subsection 19.9., "Employee Travel Related to a CHS Operation," for guidance on foreign travel in support of ET CHS activity.
- (S//NF) **CHS ET operational communications**: In support of a national security matter, a CHS, at the direction of the FBI, communicates with a subject of an investigation who is in a foreign country. The CHS may be located domestically, in the same country as the subject, or in a separate country.
- (S//NF) **Foreign-based CHS operational travel to the United States (operational-domestic travel)**: A CHS travels from a foreign country to the United States to conduct operational activity (e.g., Legat-assigned CHS operational travel to the United States to support an FO investigation, or an FO-assigned CHS who resides in a foreign country travels to the United States in support of an operation). See subsection 19.4.1.5., "Foreign-Based CHS Operational Travel to the United States (Operational-Domestic Travel."
- (S//NF) **CHS ET business or professional travel**: The CHS travels to a foreign country from the United States or from one foreign country to another foreign country for professional or business purposes and is not tasked by the FBI to collect evidence or intelligence. The CHS is not conducting business on behalf of the FBI, nor is travel paid for by the FBI. Professional or business travel can include routine travel related to the CHS's employment or profession or be part of professional development, such as attending a conference, a seminar, or a trade show. See subsection 19.4.1.7., "ET CHS Personal Travel," and subsection 19.4.1.6., "ET CHS Business/Professional Travel," for more information.
- (U//FOUO) **CHS ET personal travel**: The CHS travels to a foreign country from the United States, from one foreign country to another foreign country, or from a foreign country to the United States for personal reasons and is not tasked by the FBI to collect evidence or intelligence. The CHS's travel is not at the request of the FBI, nor is the travel paid for by the FBI. Personal travel can include activity such as a vacation, a social or familial visit to a foreign country, or travel for personal financial activity (e.g., buying vacation property). See subsection 19.4.1.7., "ET CHS Personal Travel," and subsection 19.4.1.6., "ET CHS Business/Professional Travel," for more information.

---

[9] (U) The term "foreign" refers to any body of land or water under the territorial jurisdiction of a country other than the United States. "United States" includes the District of Columbia, territories, and possessions.

- (S//NF) **CHS ET transit travel**: The purpose of this is category is solely to track the CHS travel itinerary from one foreign country to another foreign country or from one foreign country through the United States to another foreign country, as authorized in one of the other ET travel categories. Therefore, information for this category is collected as part of the ET travel request for any of the other travel categories.

(U//FOUO) The CA or co-CA must complete Delta form [redacted] whenever the CHS activity falls within the above-listed categories, except for the transit category. Completing [redacted] is required prior to:

- (U//FOUO) Conducting operational communications.
- (U//FOUO) A CHS traveling from the United States to another country to operationally support an FBI investigation.
- (U//FOUO) Operating a CHS residing in a foreign country.
- (U//FOUO) A CHS traveling from one foreign country to another foreign country or from a foreign country to the United States to operationally support an FBI investigation.

(U//FOUO) [redacted] is also used track CHS foreign personal and business/professional travel.

(U//FOUO) [redacted] is not used to seek approval for FBI employee ET travel related to a CHS operation. This is accomplished using an EC (see subsection 19.9., "Employee Travel Related to a CHS Operation"). The [redacted] is also not used to track CHS domestic personal or business/professional travel.

(U//FOUO) The previous policy on ET CHS operations used the concepts of approval for ET CHS travel and approval for ET CHS operations synonymously. This created confusion because approval is required even if a CHS does not travel, but resides and is operated in a foreign country, or if the CHS is involved in ET operational communications. This CHS operational activity authorization is mandatory regardless of the CHS's origination point (i.e., the United States or an international locale). [redacted] was updated to better define each category and provide an automated workflow for approval and notifications.

(U//FOUO) An open full investigation is required for the FBI to engage in ET CHS operations.

(U//FOUO) Subsection 7.6., "Sworn Law Enforcement Officers," contains a prohibition on opening a LEO as a CHS unless the person is reporting on matters related to public corruption. This prohibition applies only to U.S. LE personnel; no prohibition exists for foreign LEOs. However, agents must be cognizant of other sensitivities inherent in opening and tasking a foreign LEO as a CHS overseas and be aware of the definition of "foreign official" and whether or not the term applies to the LEO.

## 19.1. (U) National Security Investigations

### 19.1.1. (U) ET CHS Operation in Support of a National Security Investigation

(S//NF) The FBI may engage in the following ET activities in support of an open full substantive national security investigation or a full PFI investigation.

- (S//NF) Complete the assessment or recruitment of officials of threat countries if the assessment or recruitment was begun by the FBI in the United States.
- (S//NF) Operate and pay officials of threat countries abroad who have been recruited or operated as CHSs by the FBI in the United States, when it is not practicable to turn them over to another intelligence agency. The determination of a turnover is not based solely on practicability, but rather, on the totality of the CHS operational circumstances, including the reasonableness of the FBI's continued operation and payment of a CHS.
- (S//NF) Operate and pay CHSs traveling in response to instructions from foreign intelligence services or international terrorists.
- (S//NF) Operate and pay CHSs to travel abroad at the direction of the FBI to make contact with foreign intelligence services or international terrorists.
- (S//NF) Authorize CHSs to operate sub-sources internationally, in accordance with subsection 19.1.7., "Use of an ET Sub-Source."

### 19.1.2. (U) Prohibited ET National Security CHS Operations

(S//NF) The FBI may not engage in the following activities:

- (S//NF) Recruit as CHSs officials of countries that are not threat countries.[10] This prohibition does not apply to nonmanagement (i.e., first-line level) LEOs or other first-line-level government employees. However, if there is a question about any other LE or governmental position, the FBI agent must consult the OGC to determine whether that person falls within the meaning of "officials" as stated in this paragraph and below.
- (S//NF) Pay foreign officials, directly or indirectly, for investigative assistance. This does not preclude reimbursement of LE or security agencies of foreign governments to the extent authorized by the United States and foreign law and does not exclude the payment of a foreign LEO or national security agency employee, while the individual is open as a domestic FBI CHS, in support of an open FBI investigation (e.g., the Foreign-Domestic Security Service Initiative).

(S//NF) A foreign official is defined as a foreign national in the United States who is acting in an official capacity for a foreign power; is attached to a foreign diplomatic establishment, foreign consulate establishment, or other establishment under the control of a foreign power; or employed by an international organization or other organization under an agreement to which the United States is a party (see the NSIG).

19.2. [redacted]

[redacted]

[10] (U) See DIOG Appendix G, *Classified Provisions*, for a list of threat countries.

[redacted]

[redacted]

[redacted]

### 19.2.1. (S//NF) ET OIA by a CHS in Support of a National Security Investigation

(U//FOUO) In addition to the approval sought for an ET CHS operation in support of a national security investigation, additional approvals are required if the CHS will engage in OIA. These are set out in subsections 19.2.1.2., 19.2.1.3., and 19.2.1.4. below. The approval of the OIA may be sought concurrently with the ET operational approval request. However, if the need for OIA approval arises after CHS ET operational approval has been obtained, the OIA approval must be sought independently and obtained prior to the CHS engaging in the OIA.

(S//NF) For ET CHS national-security-related operations, OIA is defined as any activity that would constitute a crime under federal, state, or local law if engaged in by a private person, except as authorized under this policy.

(U//FOUO) In approving the OIA, FBI officials must find that the OIA is necessary to accomplish any of the following:

- (U//FOUO) Obtain significant intelligence or international terrorism information.
- (U//FOUO) Establish or maintain credibility or cover that is important to the success of an investigation.
- (U//FOUO) Prevent or avoid physical injury to individuals or serious damage to property.

(U//FOUO) FBI officials must also find that the need for the OIA outweighs its seriousness and adverse consequences.

(U//FOUO) An FBI employee must never authorize a CHS to participate in any act of violence, except that the CHS may take reasonable measures of self-defense in an emergency situation to protect his or her own life or the lives of others against wrongful force.

(S//NF) The FBI is not permitted to task a CHS operated jointly with another USG agency to perform OIA activity without the authorization required in this section. If the other agency has tasked and authorized a CHS to engage in OIA, but the FBI has not received the authorization required by this section, the FBI may otherwise continue to operate the joint CHS and participate in all aspects of the operation, including tasking, gathering intelligence, and debriefing the CHS, except that the FBI may not participate in the tasking, the conduct, or the funding of the other agency's OIA.

(U//FOUO) See subsection 19.13., "Emergency ET OIA Authorization," and subsection 19.14., "Duration of ET OIA Authorization and Request for Renewal," for guidance on these topics.

#### 19.2.1.1. (S//NF) ET OIA That Violates Federal Law or is a Felony or a Serious Crime Under State or Local Law

(U//FOUO) The following approvals are required for ET OIA in support of a national security investigation if the OIA violates any federal law or is a felony or a serious crime under state or local law:

- (U//FOUO) SAC approval of the OIA

- (U//FOUO) Appropriate IOD geographic unit and Legat notification of OIA (See also subsection 19.7, "Role of the International Operations Division in ET CHS Operations," and subsection 19.8, "ET CHS Operations by a Legat or an ALAT.")
- (U//FOUO) FBIHQ operational division AD (or designee) approval of the OIA
- (U//FOUO) AAG, NSD (or designee) approval of the OIA

(U//FOUO) For OIA related to material support for terrorism in national security investigations, see DIOG subsection 17.6 and the *Counterterrorism Policy Directive and Policy Guide*, 0775DPG, subsection 12.6.2.

(U//FOUO) [redacted] must be used to approve the ET CHS operation and has an OIA checkbox to indicate that OIA is part of the operational request. The OIA checkbox must be used if OIA is involved, but does not provide the approval authorization. Rather, the CA or co-CA must use an EC referencing the serialized [redacted] to document the approving official's finding and approval of the OIA. Moreover, since this OIA requires SAC and both FBIHQ and DOJ approvals, it is important that the requesting SA provide relevant information about the nature and scope of the proposed CHS OIA in the requesting communication, including the type(s) of violation, how the OIA advances the investigation, details of the investigation to date, and the objective(s) of the ET operation.[12] The approved EC request must be placed into the CHS OIA sub-file. OIA is not permitted in PFI investigations.

### 19.2.1.2. (S//NF) OIA That Does Not Violate Federal Law and is Not a Felony or a Serious Crime Under State or Local Law

(S//NF) SAC approval is required for OIA in which a CHS supports an ET national security operation and the activity does not violate federal law or constitute a felony or a serious crime under state or local law.[13]

(U//FOUO) [redacted] must be used to approve the ET CHS operation and has an OIA checkbox to indicate that OIA is involved with the operational request. The OIA checkbox must be used if OIA is involved, but does not provide the approval authorization. Rather, the CA or co-CA must use an EC referencing the serialized [redacted] to document the approving official's finding and approval of the OIA. The SA seeking the OIA approval must provide relevant information to the SAC about the nature and scope of the proposed CHS OIA on the Delta OIA form or in a requesting EC, including the type of violation(s), how the OIA advances the investigation, details of the investigation to date and the objective(s) of the ET operation.[14] The approved EC request must be placed into the CHS

---

[12] (U//FOUO) A sample ET OIA request template has been crafted to assist the field with writing the OIA request. The information requested in the template should be included in the Delta OIA form or in an EC tied to the overall operational approval request. The OIA template can be found in the Sentinel application under the [redacted] This template was specifically designed to expedite the ET operation OIA request.

[13] (S//NF) The language involving a felony or a serious crime under state or local law is taken from the [redacted] on OIA in national security matters. The likelihood that activity overseas would trigger a violation of state or local law is extremely small, if existent.

[14] (U//FOUO) See Note #5.

OIA sub-file. Even though the SAC is permitted to approve the OIA under this subsection, the OIA approval documentation must be included as part of the overall ET CHS operation approval request sent to FBIHQ. OIA is not permitted in PFI investigations.

(S//NF) An SAC may approve OIA in a national security CHS ET operation, including, but not limited to, establishing, funding, and maintaining secure cover by making false representations to third parties to conceal true personal identity or the true ownership of a proprietary. When such false representations are made to an employee or a component of a USG agency, an appropriate office within that agency must be notified, unless doing so would jeopardize the operation. Any decision to withhold advisement to that agency of the false representation must be made by the SAC and the AD of the FBIHQ operational division with program oversight of the investigation; the AD, in turn, must consult with DOJ, NSD on the operational factors associated with withholding the disclosure of the false representation to the USG agency.

### 19.2.1.3. (U//FOUO) Verbal DOJ Counterterrorism Section (CTS) Authorization for Certain OIA Related to Material Support of Terrorism in Counterterrorism Investigations

(U//FOUO) See DIOG subsection 17.6 for guidance on this authorization.

### 19.2.1.4. (U//FOUO) Positive Foreign Intelligence Investigations

(U//FOUO) The AGG-Dom defines foreign intelligence as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorists." A "foreign intelligence requirement" is a collection requirement issued under the authority of the Director of National Intelligence (DNI) and adopted by the DI. Additionally, the President of the United States, a USIC official designated by the President, the AG, the DAG, or other designated DOJ official may levy a foreign intelligence requirement on the FBI. Foreign intelligence collection by the FBI is based upon the issuance of such requirements.

(U//FOUO) The FBI, pursuant to Section 9 of the DIOG, places foreign intelligence requirements into one of two categories: (1) those that address national security issues that are within the FBI's core national security mission (i.e., FBI collection requirements) and (2) information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists, which are not within the FBI's core national security mission.

(U//FOUO) Requirements that fall into the second category are known as PFI collection requirements and may only be addressed under the policy for PFI in Section 9 of the DIOG.

(U//FOUO) PFI investigations, by definition, are not national security investigations, because national security investigations are within the FBI's core national security mission. However, in the interest of consistency in policy, when feasible, ET CHS operations in support of full PFI investigations follow the same approvals and notifications as those mandated for national security investigations (as described in subsection 19.2., "Required Approvals and Notifications for ET CHS National Security Operations") and are managed by the [redacted] HOC, or a designated entity.

(U//FOUO) OIA is not authorized in support of a PFI investigation.

## 19.3. (U) Criminal Investigations

(S//NF) The FBI may engage in ET CHS activities in support of an open full substantive criminal investigation.

(U//FOUO) ET CHS operations in support of criminal investigations are categorized as either involving sensitive circumstances or not involving sensitive circumstances. If the investigation involves sensitive circumstances, additional approvals apply. See subsection 19.3.2., "ET CHS Operations in Support of Criminal Investigations Involving Sensitive Circumstances."

(S//NF) For the purposes of ET CHS operations in support of criminal investigations, the following definitions apply:

- (S//NF) A foreign decision-making official is an individual with vested decision-making authority on a national level.
- (S//NF) A foreign official is a person invested with the authority of an office of a foreign nation.

(U//FOUO) This definition of foreign official in support of a criminal investigation is different from the definition of foreign official in the context of a national security investigation.

### 19.3.1. (U) ET CHS Operations in Support of Criminal Investigations Not Involving Sensitive Circumstances

(U//FOUO) The following ET CHS operations do not involve sensitive circumstances:

- (U) Authorizing CHSs to travel to and operate in foreign countries.
- (S//NF) Making reasonable payments for services and expenses to CHSs, including foreign officials who are not foreign decision-making officials (as defined in the [redacted]
- (S//NF) Expending reasonable sums for expenses associated with the debriefing or operation of foreign decision-making officials, as defined in the [redacted] (However, no payments may be made to foreign decision-making officials for services without the approval of the AG or a designated DOJ official.)
- (S//NF) Authorizing CHSs to engage in OIA not involving a sensitive circumstance, as described in subsection 19.3.4.1., "ET OIA Not Involving Sensitive Circumstances in Support of a Criminal Investigation," and approved in accordance with subsection 19.3.4.2., "Approval and Notifications for ET OIA Not Involving Sensitive Circumstances in Support of a Criminal Investigation."

### 19.3.2. (U) ET CHS Operations in Support of Criminal Investigations Involving Sensitive Circumstances

(S//NF) ET CHS operations that involve sensitive circumstances include:

- (S//NF) Developing or operating a foreign decision-making official as a CHS.

- (S//NF) Engaging in an activity that will have a significant effect on, or constitute a significant intrusion into, the legitimate operation of a foreign governmental entity.
- (S//NF) Engaging in an activity that will involve a significant risk of bodily harm, death, or a substantial financial loss to any victim.
- (S//NF) Engaging in any OIA involving any foreign decision-making official.
- (S//NF) Establishing any relationships with members of groups engaged in violent activities directed against the government then in power in the host country.
- (S//NF) Engaging in the sale of drugs in which the actual possession of the drugs is transferred in a host country, to a person who is not cooperating with the U.S. or foreign LE officials.
- (S//NF) Using as a CHS an attorney, a clergyman, a physician, or a member of the news media licensed in the United States in his or her professional capacity.
- (S//NF) Accepting money or any other item of value that is reasonably believed to be the proceeds of an illegal activity or is used in furtherance of an illegal activity.
- (S//NF) Engaging in any other activity that may have a significant adverse impact on foreign relations or LE activities with any country or group of countries, or any activity that reasonably could, if disclosed, be expected to cause significant diplomatic, governmental, or public controversy.
- (S//NF) Engaging in any OIA, except for the OIA categories listed in subsection 19.3.1., "ET CHS Operations in Support of Criminal Investigations Not Involving Sensitive Circumstances."

### 19.3.3. (U) Required Approvals and Notifications for ET CHS Criminal Operations

(U//FOUO) The request for approval of an ET CHS criminal operation is initiated by the CA or co-CA using [redacted] and approved in accordance with the below guidance. Upon serialization in Delta, the form is ingested into Sentinel and information leads are sent [redacted] to the Legat(s), the appropriate IOD geographic unit, the FBIHQ operational division unit with program responsibility, and the DI HCC, and an action lead is set to the relevant FBIHQ operational division HOC (or designee).

(U//FOUO) The standard for approving the ET CHS criminal operation is that it must be reasonably necessary to detect, investigate, prosecute, or prevent criminal conduct that is in violation of the laws of the United States. Moreover, the operation must be conducted in a manner that respects, to the greatest extent possible, the laws of the host country.

(S//NF) As part of an ET CHS criminal operation, a foreign LE official who has significant supervisory responsibility within the host country must be informed and must concur with the CHS operation. If the FO determines, in consultation with the operational division HOC and the affected Legat(s), that the host country should not be notified of the operation, articulable facts must exist showing (1) the particular circumstances within the host country jeopardize operational security, including the safety of the CHS, or (2) because of the nature of the FBI investigation, cooperation with the host country is not practical and the ET CHS operation is needed to further a compelling LE interest.

(U//FOUO) The CFP, normally the U.S. Attorney or designee, must be aware of the proposed operation if the CHS is required to testify and, so far as the operation relates to compliance with U.S. laws and prosecutive strategy, must concur with the proposed use of a CHS.

(S//NF) The CHS must be properly admonished prior to the ET operation, in accordance with subsection 19.11., "Pre-Operational CHS ET Briefs and Planning."

(U//FOUO) All ET CHS criminal operations require:

- (U//FOUO) SAC approval of the operation. This approval is an acknowledgement that the use of a CHS in the ET jurisdiction is required to further an important LE interest of the United States.
- (U//FOUO) FBIHQ operational division AD or designee approval of the operation.
- (U//FOUO) Appropriate IOD geographic unit and Legat notification of the operation (see also subsection 19.7., ""Role of the International Operations Division in ET CHS Operations").
- (S//NF) CIA Headquarters notification of the operation. The Sentinel ET CHS workflow process allows for a restricted communication to CIA Headquarters for CIA notification. The extent and timing of the COS briefing on the ET operation is determined by the Legat.
- (S//NF) COM notification of the operation, if appropriate (as determined by the Legat and the FBIHQ operational division HOC [or its functional equivalent]).

(S//NF) The COM is a DOS appointed position, either as a political appointee or as a career FSO. In either case, the COM is not a senior LE official; consequently, the COM may not understand the nature of CHS operations or the sensitivities that surround these operations. Therefore, it is critical that the Legat, FBIHQ, and the affected FO(s) coordinate closely on the COM notification process.

(S//NF) The operation of a CHS by a LEGAT, an ALAT, or an FBI task force member while in a foreign country must be approved in accordance with subsection 19.8., "ET CHS Operations by a Legat or an ALAT." For approval purposes, the IOD DAD approval corresponds to the SAC approval listed above; however, the LEGAT, ALAT, or FBI overseas task force ET CHS operation must also receive approval from the AD of the FBIHQ operational division with program oversight of the investigation the CHS is supporting. See subsection 19.7.1., "International Operations Division Approval and Management Role Over Legat- or ALAT-Assigned ET CHS," for the list of equivalent IOD approval levels.

#### 19.3.3.1. (S//NF) Additional Approvals for ET CHS Criminal Operations Involving Sensitive Circumstances

(S//NF) ET CHS criminal operations that involve sensitive circumstances require AG (or designee) approval, in addition to the approvals listed above.

(S//NF) The FBIHQ operational division HOC managing the ET request must provide the DOJ approving official with an AD-approved summary of the ET CHS criminal operation, in a document suitable for dissemination (e.g., an LHM) that sets out the relevant details of the operation, demonstrates that the standards for approving the operation have been met as set out in subsection 19.3.3. ("Required Approvals and Notifications for ET CHS Criminal Operations").

and fully explains all factors surrounding the sensitive circumstances. Once approved, a copy of the approval documentation must be placed into the CHS Delta file.

### 19.3.4. (S//NF) ET OIA by a CHS in Support of a Criminal Investigation

(S//NF) In addition to the approval sought for the ET CHS operation in support of a criminal investigation, separate approvals are required if the CHS will engage in OIA. The approval of the operation may be sought concurrently with OIA approval. However, if the need for OIA authority arises after CHS ET operational approval has been obtained, the OIA approval must be sought and obtained prior to engaging in the OIA.

(S//NF) For ET CHS criminal operations, OIA involves acts that, if engaged in by a private person, would be in violation of U.S. federal, state, or host country law without the authorization provided for in this policy. Per the applicable AGGs, OIA approval must sought if the CHS will engage in conduct in violation of host country law in support of a criminal investigation.

(U//FOUO) An FBI employee must never authorize a CHS to participate in any act of violence, except that the CHS may take reasonable measures of self-defense in an emergency situation to protect his or her own life or the lives of others against wrongful force.

(U//FOUO) See subsection 19.13., "Emergency ET OIA Authorization," and subsection 19.14., "Duration of ET OIA Authorization and Request for Renewal," for guidance on these topics.

#### 19.3.4.1. (S//NF) ET OIA Not Involving Sensitive Circumstances in Support of a Criminal Investigation

(S//NF) The following types of illegal activity, by themselves, do not constitute sensitive circumstances:

- (S//NF) Engaging in the expression of intent to participate in criminal activity
- (S//NF) Engaging in illegal gambling activities
- (S//NF) Engaging in controlled purchases of stolen property, provided that measures are undertaken to ensure that the property, once delivered, will not leave the care, custody, or control of the U.S. or foreign LEOs
- (S//NF) Engaging in controlled purchases of contraband, including drugs, weapons, and explosives, provided that measures are undertaken to ensure that the contraband, once delivered, will not leave the care, custody, or control of the U.S. or foreign LEOs
- (S//NF) Engaging in the controlled delivery of contraband, including drugs, weapons, and explosives, into the United States, provided that domestic guidelines and procedures with respect to the controlled delivery of drugs or other dangerous contraband in the United States are followed

#### 19.3.4.2. (U//FOUO) Approval and Notifications for ET OIA Not Involving Sensitive Circumstances in Support of a Criminal Investigation

(U//FOUO) All ET CHS OIA not involving sensitive circumstances conducted in support of a criminal investigation requires:

- (U//FOUO) SAC approval of the OIA.

- (U//FOUO) Appropriate IOD geographic unit and Legat notification of the OIA (see also subsection 19.6., "Role of the Legat in ET CHS Operations," and subsection 19.7., "Role of the International Operations Division in ET CHS Operations")
- (U//FOUO) FBIHQ operational division AD (or designee) approval of the OIA

(S//NF) By approving the OIA, the approving officials are acknowledging their finding that the benefits of the operation outweigh the risks associated with the CHS engaging in such activity.

(U//FOUO) [redacted] must be used to approve the ET CHS operation and has an OIA checkbox to indicate that OIA is part of the operational request. The OIA checkbox must be used if OIA is involved, but does not provide the approval authorization. Rather, the CA or co-CA must use an EC referencing the serialized [redacted] to document the approving official's finding and approval of the OIA. Moreover, since this OIA requires SAC and FBIHQ approval, it is important that the requesting SA provide relevant information about the nature and scope of the proposed CHS OIA in the requesting communication, including the type(s) of violation, how the OIA advances the investigation, details of the investigation to date, and the objective(s) of the ET operation.[15] The approved EC request must be placed into the CHS OIA sub-file.

#### 19.3.4.3. (S//NF) ET OIA Involving Sensitive Circumstances in Support of a Criminal Investigation

(S//NF) If the ET CHS OIA does not fall within the limited list of nonsensitive OIA listed in subsection 19.3.4.1., "ET OIA Not Involving Sensitive Circumstances in Support of a Criminal Investigation," the OIA is deemed sensitive.

#### 19.3.4.4. (S//NF) Approval and Notifications for ET OIA Involving Sensitive Circumstances in Support of a Criminal Investigation

(S//NF) The following approvals and notifications are required for a CHS to engage in ET OIA that involves sensitive circumstances:

- (U//FOUO) SAC approval of the OIA
- (U//FOUO) Appropriate IOD unit and Legat notification of the operation (see also subsection 19.6., "Role of the Legat in ET CHS Operations," and subsection 19.7., "Role of the International Operations Division in ET CHS Operations")
- (U//FOUO) FBIHQ operational division AD (or designee) approval of the OIA
- (U//FOU) DOJ, Criminal Division, Office of International Affairs approval of the OIA

(S//NF) By approving the OIA, the approving officials are acknowledging their finding that the benefits of the operation outweigh the risks associated with the CHS engaging in such activity.

---

[15] (U//FOUO) A sample ET OIA request template has been crafted to assist the field with writing the OIA request. The information requested in the template should be included in the Delta OIA form or in an EC tied to the overall operational approval request. The OIA template can be found in the Sentinel application under the "Bookmarks" section, [redacted]. This template was specifically designed to expedite the ET operation OIA request.

(U//FOUO) [redacted] must be used to approve the ET CHS operation and has an OIA checkbox to indicate that OIA is involved with the operational request. The OIA checkbox must be used if OIA is involved, but does not provide the approval authorization. Rather, the CA or co-CA must use an EC referencing the serialized [redacted] to document the approving official's finding and approval of the OIA. Since this OIA requires SAC and both FBIHQ and DOJ approvals, it is important that the requesting SA provide relevant information about the nature and scope of the proposed CHS OIA in the requesting EC, including the type(s) of violation, how the OIA advances the investigation, details of the investigation to date, and the objective(s) of the ET operation.[16] The approved EC request must be placed into the CHS OIA sub-file.

### 19.4. (U) Policy Applicable to ET CHS Operations in Support of All Types of Investigations

(U//FOUO) Use of [redacted] is required each time a CHS engages in ET operational travel or an ET operational activity (i.e., to seek a "one-time" authorization). However, a period of authorization may be used for any travel/ET activity authorization type and should be selected when a CHS resides in, or travels frequently (i.e., more than three times during a consecutive 30-day period) to and from the same country, so long as the operational scope, techniques used, or geographic region does not change during that period. [redacted] must be used regardless of the CHS's origination point (i.e., the United States or an international locale, in cases in which a CHS resides in a foreign country). This form must also specify the specific nature of the operational travel or activity. The exemption to reporting each operational travel request is in place to recognize situations such as CHS travel near or on the border of Mexico, Canada, or any other frequent cross-border travel area, and the CHS's CA or co-CA must closely coordinate this exemption with the FBIHQ operational division HUMINT Operations Center (HOC) and the affected Legat.

#### 19.4.1. (U) Documentation Requirements for All CHS ET Operational and Communication Requests

##### 19.4.1.1. (S//NF) CHS ET Operational Travel

(S//NF) Whenever a CHS travels to a foreign country from the United States or from one foreign country to another foreign country to engage in operational activity (e.g., when tasked to collect intelligence or evidence) on behalf of the FBI, the CA or co-CA must complete [redacted] All communications with an ET CHS must be requested using the communication section of [redacted] and be approved as part of the CHS ET operation.

(S//NF) [redacted] must be filled out in its entirety. The selection within the "CHS Activity Details" field directs the user to provide relevant information. The request must set out the justification for seeking ET operational authority, include all pertinent facts and the background of the investigation, and describe how the ET operation furthers the prosecutorial or intelligence objectives of the investigation. The request must acknowledge, when appropriate, that the AUSA or DOJ attorney, if assigned, supports the use of the CHS in the ET operation.

---

[16] (U//FOUO) See previous note.

Upon completion, the form is serialized in Delta and the information is imported and sent via [redacted] to relevant FBIHQ stakeholders in Sentinel restricted case files.

(U//FOUO) For example, if "Extraterritorial Operational" is selected as a category in the "CHS Travel/ET Activity" field and the [redacted] is approved and serialized in Delta, the automated Delta/Sentinel workflow will:

- (U//FOUO) Set an action lead to the relevant FBIHQ operational division HOC (to complete the FBIHQ coordination, authorization, and notification process).
- (U) Set an information lead to the operational division UC with program responsibility over the CHS operation (selected by the drafter of the [redacted]).
- (U) Set an information lead to Legat(s) (determined from routing table, by country).
- (U) Set an information lead to the appropriate IOD geographic unit (determined from routing table, by country).
- (U) Set an information lead to the HCC.

(U) In support of the above, the completed [redacted] will be routed to restricted files in Sentinel.

(S//NF) The FBIHQ operational division HOC (or its functional equivalent) is responsible for obtaining additional approvals, coordinating with the relevant IOD geographic unit, and performing other tasks, as detailed in subsection 19.5., "Roles of the FBIHQ Operational Entities."

(S//NF) If OIA authorization is sought as part of the CHS ET operation, see subsection 19.2.1., "ET OIA by a CHS in Support of a National Security Investigation," and subsection 19.3.4., "ET OIA by a CHS in Support of a Criminal Investigation," for OIA approval requirements.

(S//NF) If the ET CHS operation seeks to exempt notification to the Legat(s), the requesting office must provide compelling justification and the exemption must be approved in accordance with subsection 19.15., "Exemption to Providing Legat Notification."

(S//NF) The ET operation request must clearly identify whether the operation is to be declared to the host country. In national security matters, the presumption is that the host country will not be notified of the operation. In criminal matters, if the CHS operation is not to be declared to the host country, the request must provide the justification for not informing the host country of the operation. The undeclared criminal ET operation must also be coordinated with the division HOC and the appropriate Legat in accordance with subsection 19.5.1., "Role of the Operational Division HUMINT Operations Center," and subsection 19.6., "Role of the Legat in ET CHS Operations."

(S//NF) If the operation is to be conducted jointly with the host country or with other USG agencies in the host country, the [redacted] submission must provide details on the nature and scope of the joint operation. Should the ET operation be conducted as a unilateral operation, the FBI's exclusive operation of the CHS must be detailed in the request as well.

(U//FOUO) Use of [redacted] is required each time a CHS engages in ET operational travel or an ET operational activity (i.e., to seek a "one-time" authorization). See subsection

19.4., "Policy Applicable to ET CHS Operations in Support of All Types of Investigations," for further details.

(U//FOUO) The CA or co-CA must communicate an emergency communication plan, as detailed in the [redacted] to a CHS traveling for operational reasons.

#### 19.4.1.2. (S//NF) CHS ET Resident

(S//NF) Whenever the CA or co-CA opens a CHS who is a resident of a foreign country, the CA must document this fact using [redacted]. The CA or co-CA must detail CHS taskings to engage in operational communication with persons in other foreign countries using the communication section of the [redacted] and have these approved as part of the CHS ET operation. This information is particularly important for an ET resident CHS, since tasking, debriefing, and operational and emergency communication strategies must be carefully planned and fully understood by the CHS.

(S//NF) The [redacted] must be filled out in its entirety. The selection within the "CHS Activity Details" directs the user to provide relevant information. The request must set out the justification for seeking ET operational authority, include all pertinent facts and background of the investigation, and detail how the ET operation furthers the prosecutorial or intelligence objectives of the investigation. The request must acknowledge that the AUSA or DOJ attorney, if assigned, supports the ET operation. Upon completion, the [redacted] is serialized in Delta and the information is imported and [redacted] to relevant FBIHQ stakeholders in Sentinel restricted case files.

(U//FOUO) For example, if "Resident," is selected as a category in the "CHS Travel/ET Activity" field and the [redacted] is approved and serialized in Delta, the automated Delta/Sentinel workflow will:

- (U//FOUO) Set an action lead to the relevant FBIHQ operational division HOC (to complete the FBIHQ coordination, authorization, and notification process).
- (U) Set an information lead to the operational division UC with program responsibility over the CHS operation (selected by the drafter of the [redacted]).
- (U) Set an information lead to Legat(s) (determined from routing table, by country).
- (U) Set an information lead to the appropriate IOD geographic unit (determined from routing table, by country).
- (U) Set an information lead to the HCC.

(U) In support of the above, the completed [redacted] will be routed to restricted files in Sentinel.

(S//NF) The FBIHQ operational division HOC (or its functional equivalent) is responsible for obtaining additional approvals, coordinating with the relevant IOD geographic unit, and performing other tasks, as described in subsection 19.5.1., "Role of the Operational Division HUMINT Operations Center."

(S//NF) If OIA authorization is sought, see subsection 19.2.1, "ET OIA by a CHS in Support of a National Security Investigation," and subsection 19.3.4, "ET OIA by a CHS in Support of a Criminal Investigation," for OIA approval requirements.[17]

(S//NF) If the ET CHS operation seeks to exempt notification to the Legat(s), the requesting office must provide compelling justification and the exemption must be approved in accordance with subsection 19.15, "Exemption to Providing Legat Notification."

(S//NF) The ET operation request must clearly identify whether the operation is to be declared to the host country. In national security matters, the presumption is that the host country will not be notified of the operation. In criminal matters, if the CHS operation is not to be declared to the host country, the request must provide the justification for not informing the host country of the operation. The undeclared criminal ET operation must also be coordinated with the division HOC and the appropriate Legat in accordance with subsection 19.5.1, "Role of the Operational Division HUMINT Operations Center," and subsection 19.6, "Role of the Legat in ET CHS Operations."

(S//NF) If the operation is to be conducted jointly with the host country or with other USG agencies in the host country, the [redacted] submission must provide details on the nature and scope of the joint operation. Should the ET operation be conducted as a unilateral operation, the FBI's exclusive operation of the CHS must be detailed in the request as well.

(U//FOUO) The CA or co-CA must communicate an emergency communication plan, as detailed in the [redacted] to a CHS who is a resident of a foreign country.

### 19.4.1.3. (S//NF) CHS ET Debrief

(S//NF) This category applies whenever a CHS travels at the request of the FBI to meet in a foreign country for a debriefing, for training, to receive passed items or be assessed. The CA or co-CA must document such activity using the [redacted] The manner of communication with an ET CHS must be specified using the communication section of the [redacted] and approved as part of the CHS ET operation.

(S//NF) The [redacted] must be filled out in its entirety. The selection within the "CHS Activity Details" field directs the user to provide relevant information for the selected category. The request must set out the justification for seeking ET operational authority, and include all pertinent facts and the background of the investigation, and describe how the ET operation furthers the prosecutorial or intelligence objectives of the investigation. The request must acknowledge that the AUSA or DOJ attorney, if assigned, supports the ET operation. Upon completion, the [redacted] is serialized in Delta and the information is imported and [redacted] to relevant FBIHQ stakeholders in Sentinel restricted case files.

---

[17] (U//FOUO) A sample ET OIA request template has been crafted to assist the field with writing the OIA request. The information requested in the template should be included in the Delta OIA form or in an EC tied to the overall operational approval request. The OIA template can be found in the Sentinel application, under the "Bookmarks" section, in the [redacted] This template was specifically designed to expedite the ET operation OIA request. The approved EC request must be placed into the CHS OIA sub-file.

(U//FOUO) For example, if "Third Country Debrief" is selected as a category in the "CHS Travel/ET Activity" field and the [redacted] is approved and serialized in Delta, the automated Delta/Sentinel workflow will:

- (U//FOUO) Set an action lead to the relevant FBIHQ operational division HOC (to complete the FBIHQ coordination, authorization, and notification process)
- (U) Set an information lead to the operational division UC with program responsibility over the CHS operation (selected by the drafter of the [redacted])
- (U) Set an information lead to Legat(s) (determined from routing table, by country)
- (U) Set an information lead to the appropriate IOD geographic unit (determined from routing table, by country)
- (U) Set an information lead to the HCC.

(U) In support of the above, the completed [redacted] will be routed to restricted files in Sentinel.

(S//NF) The FBIHQ operational division HOC (or its functional equivalent) is responsible for obtaining additional approvals, coordinating with the relevant IOD geographic unit, and performing other tasks, as described in subsection 19.5.1., "Role of the Operational Division HUMINT Operations Center."

(S//NF) If OIA authorization is sought, see subsection 19.2.1., "ET OIA by a CHS in Support of a National Security Investigation," and subsection 19.3.4., "ET OIA by a CHS in Support of a Criminal Investigation," for OIA approval requirements.[18]

(S//NF) If the ET CHS operation seeks to exempt notification to the Legat(s), the requesting office must provide compelling justification and the exemption must be approved in accordance with subsection 19.15., "Exemption to Providing Legat Notification."

(S//NF) The ET operation request must clearly identify whether the operation is to be declared to the host country. In national security matters, the presumption is that the host country will not be notified of the operation. In criminal matters, if the CHS operation is not to be declared to the host country, the request must provide the justification for not informing the host country of the operation. The undeclared criminal ET operation must also be coordinated with the division HOC and the appropriate Legat in accordance with subsection 19.5.1., "Role of the Operational Division HUMINT Operations Center," and subsection 19.6., "Role of the Legat in ET CHS Operations."

(S//NF) If the operation is to be conducted jointly with the host country or with other USG agencies in the host country, the [redacted] submission in Delta must provide details on the nature and scope of the joint operation. Should the ET operation be conducted as a unilateral operation, the FBI's exclusive operation of the CHS must be detailed in the request as well.

---

[18] (U//FOUO) A sample ET OIA request template has been crafted to assist the field with writing the OIA request. The information requested in the template should be included in the Delta OIA form or in an EC tied to the overall operational approval request. The OIA template can be found in the Sentinel application under the "Bookmarks" section, at the [redacted] This template was specifically designed to expedite the ET operation OIA request. The approved EC request must be placed into the CHS OIA sub-file.

(U//FOUO) The CA or co-CA must communicate an emergency communication plan to a CHS, as detailed in the [redacted] to any CHS in this category.

### 19.4.1.4. (S//NF) CHS ET Operational Communications

(S//NF) This category applies whenever a CHS, in support of a national security matter and at the direction of the FBI, communicates[19] with a subject of an investigation who is in a foreign country. The CHS may be located domestically, in the same country as the subject, or in a separate country.

(U//FOUO) Use of the [redacted] for communication with the subject of a national security investigation is required each time this type of communication is tasked. However, if a CHS frequently communicates with the same subject(s) (i.e., more than three times during a consecutive 30-day period), a single [redacted] may be used to specify a communication timeframe of up to one year, using the "Period of Authorization" category for documenting the frequent communications. This exemption from requiring an [redacted] to report each operational communication request is in place to recognize the globalization of communication technology; however, the CHS's CA or co-CA should coordinate the use of the exemption with the FBIHQ operational division HOC to discuss the geographical scope, the anticipated timeframe, and the affected countries.

(U//FOUO) The [redacted] must specify the nature of the operational communications. Also, for a "resident" CHS, if this type of subject-related communication is already included in the initial [redacted] a separate authorization is not required, as long as the scope of the communications or the geographic area remains the same. However, if the scope changes or expands, a separate authorization request must be submitted. For example, if a CHS resident in France is authorized, as part of the initial request, to communicate with a national security subject in Belgium, but later the FBI tasks the CHS with access to other known subjects and expands the operational communication to subjects in Germany and the Netherlands, another [redacted] using the CHS ET operational communications category must be submitted for approval to acknowledge the expansion of the scope of the subject communications and the geographic locations.

(S//NF) The [redacted] must be filled out in its entirety. The selection within the "CHS Activity Details" field directs the user to provide relevant information for the selected category. The request must set out the justification for seeking ET operational authority, include all pertinent facts and the background of the investigation, and describe how the ET operation furthers the prosecutorial or intelligence objectives of the investigation. The request must acknowledge that the AUSA or DOJ attorney, if assigned, supports the ET operation. Upon completion, the form is serialized in Delta and the information is imported and [redacted] to relevant FBIHQ stakeholders in Sentinel restricted case files.

(U//FOUO) For example, if "ET Communications" is selected as a category in the "CHS Travel/ET Activity" field and the [redacted] is approved and serialized in Delta, the automated Delta/Sentinel workflow will:

---

[19] A consensual recording of a foreign subject by a domestic-based CHS must be authorized by using an [redacted]

- (U//FOUO) Set an action lead to the relevant FBIHQ operational division HOC (to complete the FBIHQ coordination, authorization, and notification process).
- (U) Set an information lead to the operational division UC with program responsibility over the CHS operation (selected by the drafter of the [redacted]).
- (U) Set an information lead to Legat(s) (determined from routing table, by country).
- (U) Set an information lead to the appropriate IOD geographic unit (determined from routing table, by country).
- (U) Set an information lead to the HCC.

(U) In support of the above, the completed [redacted] will be routed to restricted files in Sentinel.

(U//FOUO) As a general rule, an employee based domestically is prohibited from contacting a CHS while the CHS is in a foreign country. This rule applies to all communications between an employee and a CHS in a foreign country, regardless of whether the employee is initiating the contact from within the United States or a foreign country. However, if communications with an ET CHS are a requirement for the success or safety of the operation, the method or type of communication must be explicity requested and then approved as part of the communication section of the [redacted]

(S//NF) In reviewing the ET operational communication request, the FBIHQ operational division HOC should consult with OTD regarding suitable methodology and available tools for the communication. See also subsection 10.2., "Electronic Communications with a CHS."

(S//NF) If the ET CHS operation seeks to exempt notification to the Legat(s), the requesting office must provide compelling justification and the exemption must be approved in accordance with subsection 19.15., "Exemption to Providing Legat Notification."

#### 19.4.1.4.1. (S//NF) In-Country Communications

[redacted]

[redacted]

(U//FOUO) The CA or co-CA must communicate an emergency communication plan, as detailed in [redacted] to a CHS, whether the CHS is traveling for operational, personal, business, or professional reasons. See subsection 10.2., "Electronic Communications with a CHS," for additional information on CHS communication techniques.

### 19.4.1.5. (S//NF) Foreign-Based CHS Operational Travel to the United States (Operational-Domestic Travel)

(U//FOUO) Whenever a CHS travels from a foreign country to the United States to conduct operational activity (e.g., a Legat-assigned CHS travels to the United States to support an FO investigation or an FO-assigned CHS who resides in a foreign country travels to the United States in support of an investigation), the CA must obtain prior concurrence from the SAC (or designee) of the receiving FO in which the operation will occur, if practicable. If not practicable, the affected FO(s) must be notified as soon as possible, but no later than five business days from the date of the operational activity. The [redacted] should be used to document the prior concurrence, or post-operation notification, of the affected FO(s). The use of the [redacted] is to document, in the CHS's file, the coordination efforts undertaken by FOs and Legats.

(U//FOUO) For example, when "Operational-Domestic Travel" is selected as a category in the "CHS Travel/ET Activity" field and the [redacted] is approved and serialized in Delta, the automated Delta/Sentinel workflow will set an information lead to the receiving FO CHSC (for situational awareness).

(U//FOUO) In support of the above, the completed [redacted] will be routed to restricted files in Sentinel.

(U//FOUO) This subsection does not apply to online operations. For CHS online operational activity known to affect another FO's AOR, coordination between affected FOs is recommended for deconfliction purposes. Coordination efforts must be documented in the CHS main file.

### 19.4.1.6. (U) ET CHS Business/Professional Travel

(U) Whenever the CHS's CA or co-CA becomes aware that a CHS plans to travel, or is traveling, outside the United States for business/professional purposes, the CA or co-CA must document the travel using [redacted] The selection within the "CHS Activity Details" field directs the user to provide relevant information for the selected category. Upon completion, the [redacted] is serialized in Delta and the information is imported and [redacted] to relevant FBIHQ stakeholders in Sentinel restricted case files.

(U//FOUO) For example, if "Business/Professional" is selected as a category in the "CHS Travel/ET Activity" field and the [redacted] is approved and serialized in Delta, the automated Delta/Sentinel workflow will:

- (U//FOUO) Set an information lead to the relevant FBIHQ operational division HOC (for situational awareness).
- (U) Set an information lead to the substantive desk UC (selected by the drafter of the [redacted] for situational awareness).
- (U) Set an information lead to the Legat (determined from routing table, by country).
- (U) Set an information lead to the appropriate IOD geographic unit (determined from routing table, by country).
- (U) Set an information lead to the HCC (for situational awareness).

(U) In support of the above, the completed [redacted] will be routed to restricted files in Sentinel.

(U//FOUO) Use of the [redacted] for business/professional ET travel is required each time a CHS travels for business/professional purposes outside the United States. See subsection 19.4., "Policy Applicable to ET CHS Operations in Support of All Types of Investigations," for further details.

(U//FOUO) If a CHS fails to notify the CA of ET business/professional travel in advance, the CA must still document the travel on the [redacted] after the fact and have it serialized into the CHS file to ensure that the information is accessible to the required stakeholders. The CA or co-CA should remind the CHS that the CHS should inform the FBI of his or her ET business/professional travel.

(U//FOUO) Business/professional post-travel CHS debriefs must not be used by CAs to circumvent the need for approval for CHS operational travel. The business/professional travel category is for business/professional travel wherein the CHS is not tasked by the FBI to collect evidence or intelligence. The CHS is not conducting business on behalf of the FBI, nor is the travel paid for by the FBI. Professional or business travel may include routine travel related to the CHS's employment or profession or be part of professional development, such as attending a conference, a seminar, or a trade show. In fact, for this category, the CA or co-CA must describe in detail on the [redacted] any possible untasked intelligence collection and/or contacts of intelligence value the CHS may encounter during this ET travel or activity. In a circumstance in which a CHS's post-business/professional-travel debriefing results in disseminable intelligence, the information must be vetted, for deconfliction purposes, with the appropriate Legat(s) prior to its dissemination via an intelligence product outside of the FBI (e.g., in an IIR).

(U//FOUO) The CA or co-CA must communicate an emergency communication plan, as detailed in the [redacted] to a CHS traveling for business or professional reasons.

### 19.4.1.7. (U) ET CHS Personal Travel

(U) Whenever the CHS's CA or co-CA becomes aware that a CHS plans to travel, or is traveling, outside the United States for personal purposes, the CA or co-CA must document the travel in [redacted] The selection within the "CHS

Activity Details" field directs the user to provide relevant information for the selected category. Upon completion, the [redacted] is serialized in Delta and the information is imported and [redacted] to relevant FBIHQ stakeholders in Sentinel restricted case files.

(U//FOUO) For example, if "Personal" is selected as a category in the "CHS Travel/ET Activity" field and the [redacted] is approved and serialized in Delta, the automated Delta/Sentinel workflow will:

- (U//FOUO) Set an information lead to the relevant FBIHQ operational division HOC (for situational awareness).
- (U) Set an information lead to the substantive desk UC (selected by the drafter of the [redacted] for situational awareness).
- (U) Set an information lead to the Legat (determined from routing table, by country).
- (U) Set an information lead to the appropriate IOD geographic unit (determined from routing table, by country).
- (U) Set an information lead to the HCC (for situational awareness).

(U) In support of the above, the completed [redacted] will be routed to restricted files in Sentinel.

(U//FOUO) Use of the [redacted] for personal ET travel is required each time a CHS travels for personal reasons outside the United States. The [redacted] must specify the specific nature of the personal travel. See subsection 19.4., "Policy Applicable to ET CHS Operations in Support of All Types of Investigations," for further details.

(U//FOUO) If a CHS fails to notify the CA of ET personal travel in advance, the CA or co-CA must still document the travel on the [redacted] after the fact and have it serialized into the CHS file to ensure that the information is accessible to the required stakeholders. The CA or co-CA should remind the CHS of the FBI's personal and business/professional travel notification requirements regarding ET nonoperational travel.

(U//FOUO) In a circumstance in which a CHS's post-personal-travel debriefing results in intelligence that can be disseminated, the information must be vetted, for deconfliction purposes, with the appropriate Legat(s) prior to its dissemination via an intelligence product outside of the FBI (e.g., in an IIR).

(U//FOUO) The CA or co-CA must communicate an emergency communication plan, as detailed in the [redacted] to a CHS traveling for personal reasons.

### 19.4.1.8. (U//FOUO) CHS ET Transit Travel

(U) The purpose of this category is to track all "legs" of travel, or the CHS travel itinerary, as the CHS travels through foreign countries. This information is collected as part of the completion of [redacted] when it is used for one of the other travel categories. Therefore, it is not necessary to complete a separate [redacted] for this category.

(U//FOUO) The CA or co-CA must communicate an emergency communication plan, as detailed in the [redacted] to the CHS for the countries through which he or she is transiting.

### 19.5. (U//FOUO) Roles of the FBIHQ Operational Entities

#### 19.5.1. (U//FOUO) Role of the Operational Division HUMINT Operations Center

(S//NF) For all ET CHS operations, the AD of the FBIHQ operational division with program responsibility over the operation must designate a HOC to receive and process the requisite approvals and notifications for ET operational requests. The HOC, or other specified entity, (e.g., CTD's Counterterrorism HUMINT Operations Unit [CHOU]) is a select group of FBI personnel assigned by the operational division to centralize the evaluation of risk associated with the CHS ET activity, standardize the approval process, represent the deconfliction of ET activity on behalf of the operational division, and serve as the single POC for communications surrounding the ET activity within the operational division.

(S//NF) The HOC (or its functional equivalent) must review the [redacted] to ensure that it is in support of an open full investigation and is reasonably necessary to detect, investigate, prosecute, or prevent criminal conduct in violation of U.S. laws; to further U.S. national security interests; or to support a PFI investigation. To do so, the HOC must:

- (S//NF) Initiate the CHS ET Activity Package and AD authorization EC within Sentinel to prepare the requisite authorization and notification documents, including, but not limited to, CIA correspondence cables, [redacted] and host-nation and/or U.S. LE partners, and the operational division's authorization EC.
- (S//NF) Ensure that the affected Legats receive notification of the operational request and, if changes are made to the itinerary, that the affected Legats and other stakeholders are provided a copy of the submitted [redacted] and added to the document review of the CHS ET Activity Package within Sentinel.
- (S//NF) Evaluate the tradecraft, communications plan, and emergency safety plan in accordance with the operating environment information and advisories managed by the HCC, in consultation with the Legat and FBIHQ operational divisions.
- (S//NF) Review the [redacted] request to ensure that it is in support of an open full substantive investigation and is reasonably necessary to detect, investigate, prosecute, or prevent criminal conduct in violation of U.S. laws; to further U.S. national security interests; or to support a PFI investigation. Examples of ET CHS operations can be found on the HCC Intranet page.
- (S//NF) Ensure that all reasonable measures have been taken to reduce the risks of physical and monetary harm arising out of the investigation.
- (S//NF) Ensure that other U.S. or host country agencies involved in the operation of the CHS, both in the United States and in the foreign country, have been identified and that their operational roles, if any, are clearly stated in the request. Additionally, ensure that all logical steps have been taken to coordinate with other ET U.S. LE agencies with which the CHS activities could conflict.
- (S//NF) Evaluate the justification for any request for exemption from Legat notification pursuant to subsection 19.15., "Exemption to Providing Legat Notification," and, if justification is deemed appropriate, coordinate the notifications of CIA and the COM

with IOD. The exemption request must be approved via an EC, not by use of the [redacted]

- (S//NF) Ensure that the ET operation request clearly identifies whether or not the operation is to be declared to the host country. In criminal matters, if the operation is not to be declared to the host country, the request must provide the justification for not informing the host country of the operation. In national security matters, the presumption is that the host country will not be notified of the operation.
- (S//NF) Ensure that CIA approvals have been obtained, as appropriate.
- (S//NF) Ensure that COM notifications have been provided, as appropriate.
- (S//NF) Ensure that declared or joint operations are properly coordinated among affected in-country agencies. This is accomplished by seeking CIA Headquarters approval or notification via a [redacted] as the official communication. A record of the request must be serialized as part of the CHS ET Activity Package and routed and retained in the appropriate restricted HOC files; the response from the CIA is routed and retained in the appropriate restricted HOC CIA cable sub-file [redacted]. A copy of the final approval must be forwarded to the CA or co-CA for inclusion in the CHS [redacted] file. The CIA Headquarters or COS approval or notification is required for unilateral and joint ET CHS operations, regardless of whether the operation is declared to the host country or is an undeclared operation.
- (S//NF) Review each request in which "ET Operational Communications" is the category used to submit the [redacted] for authorization to ensure that it meets the standards for submission (i.e., the communications are operational in nature, with a subject, and are part of an FBI tasking), is not covered by an already-submitted [redacted] and expands and accurately describes the operational communications.
- (S//NF) Coordinate with and assist the FBIHQ operational division unit in obtaining operational division AD approval, as needed, if the FO/Legat requests OIA that requires FBIHQ and DOJ approval. Additionally, in national security operations, consult with DOJ, NSD on CHS activities that involve false representations to a third party about CHS qualifications that are subject to state or federal licensing requirements.
- (S//NF) Seek AD (or designee) approval upon determining that the operation request meets operational division approval and notification requirements, as set out in this subsection and as appropriate for national security or criminal operations.
- (S//NF) Ensure that the operational and communication plan includes appropriate tradecraft to protect the CHS from subjects and/or penetration by host country intelligence services.

(S//NF) Once the AD (or his or her designee) has approved or denied the [redacted] the HOC must notify the CA of the approval or denial of the operation, including the decision justification, via the automated notification in the travel/ET activity workflow in Sentinel. Furthermore, copies of the authorization and notification documents, including, but not limited to, [redacted]

[redacted] and the AD authorization EC must be forwarded to the CA for inclusion in the CHS's Delta file.

### 19.5.2. (U//FOUO) Role of the FBIHQ Operational Unit

(S//NF) For all ET CHS operations, the FBIHQ operational unit with program responsibility over the operation must, upon receiving notification of the ET operational request:

- (S//NF) Review the request to ensure that it is in support of an open full investigation and is reasonably necessary to detect, investigate, prosecute, or prevent criminal conduct in violation of U.S. laws; to further U.S. national security interests; or to support a PFI investigation.
- (S//NF) Work with the FBIHQ operational division HOC to provide knowledge of the case objectives and evaluate any risk to the FBI involved in conducting ET operations, in accordance with the operating environment information and advisories managed by the HCC and in consultation with the Legat and all FBIHQ operational divisions.
- (S//NF) Ensure, for any OIA requested that requires FBIHQ and DOJ approval, that relevant details of the OIA are summarized in writing, approved by the operational division AD, in coordination with the FBIHQ operational unit, and communicated to DOJ using a document suitable for dissemination (e.g., an LHM).[20] In declared ET operations involving OIA, the host country government may require its relevant judicial body or court to authorize the activity that will occur within its border if the activity contravenes host country law (e.g., the purchase of narcotics from a subject). In such circumstances, close coordination among the HOC and affected Legat(s) is crucial to success. Additionally, FBIHQ operational divisions have the discretion to direct the HOC or the FBIHQ operational unit to obtain required OIA approvals.
- (S//NF) Monitor the completion of CHS ET travel/activity authorization requests in support of program-managed investigations.

### 19.5.3. (U//FOUO) Role of the Directorate of Intelligence HUMINT Coordination Center

(U//FOUO) The DI enterprise HCC serves as a HUMINT ET operations clearing house for coordination, deconfliction, standardization, and analysis of ET CHS activity. The HCC's purpose is to maximize the ET CHS data collection for executive decision makers and the transparency of ET CHS activities among operational divisions to manage operational risks and identify cross-programmatic intelligence opportunities.

(S//NF) The enterprise HCC works with each operational division HOC to centralize the evaluation of risk associated with the CHS ET activity, standardize the approval process, and facilitate the deconfliction of ET activity on behalf of all FBIHQ operational divisions, IOD, and the Legats. The HCC is the primary POC for communications involving cross-programmatic CHS travel and ET activity within the FBI and across the USIC community. Because of its cross-

---

[20] A sample ET OIA request template has been crafted to assist both the field and FBIHQ with writing the OIA request for approval. Although this template's use is not mandatory, it can assist with providing the approving official with the information necessary to make an informed finding quickly. Moreover, it was designed to address common themes and issues DOJ raised in prior operational settings. The template can be found in the Sentinel [redacted]

programmatic coordination capability, the enterprise HCC also serves as the central coordination point on ET-related CHS issues for the USIC and other governmental agencies and services. Additionally, the enterprise HCC is the principal FBIHQ entity for collecting, analyzing, and producing metrics and reports on CHS travel and ET activity across all operational programs.

(U//FOUO) For all CHS travel and ET activity, the HCC must:

- (U//FOUO) Ensure that information collected in Delta and transmitted in Sentinel is routed via restricted Sentinel case files to the relevant stakeholders, as determined in conjunction with the FOs and FBIHQ operational divisions.
- (U//FOUO) Coordinate the deconfliction of CHS travel and ET activity across all FBIHQ operational divisions.
- (S//NF) Manage the information and advisories for tradecraft, communications plans, and emergency safety plans in consultation with IOD, the Legats, and FBIHQ operational divisions, as appropriate for each Legat's operating environments.
- (S//NF) Work with IOD, the Legats, and FBIHQ operational divisions to ensure that appropriate tradecraft is utilized within each country and communicate operating environment changes to FBIHQ operational divisions and FOs.

### 19.6. (U//FOUO) Role of the Legat[21] in ET CHS Operations

(U//FOUO) A Legat must, upon receipt of a request for ET CHS operation:

- (S//NF) Provide guidance regarding current cooperation, treaties, and agreements with the host country which might be adversely affected if the proposed CHS operation were publically exposed or which might otherwise affect the ability to operate the CHS in the host country.
- (S//NF) Provide guidance regarding host country laws; communication protocols, such as the emergency communication of threat information; the state of the operating environment, including capabilities of the host country intelligence service(s), current local threats; the availability of safe houses or CHS safe meeting locations, if needed; and other matters that may have an impact on the proposed travel and operation of the CHS.
- (S//NF) Coordinate with the COS on all CHS activity, as appropriate.
- (S//NF) Make a determination, in coordination with the FO and the FBIHQ operational division HOC, regarding the extent of COM notification of operational activities, consistent with embassy protocols and in accordance with 22 U.S.C. § 3927(b).
- (S//NF) Provide the appropriate IOD geographic unit with input and guidance regarding the feasibility and advisability of the proposed operation.
- (S//NF) Notify the appropriate host country LE authority and coordinate the requirements of any CHS travel and ET activity operation, including authorization to engage in activities that may be illegal in the host country (e.g., seek host country judicial authority

[21] If no Legat covers a foreign geographical area, the IOD geographic unit with management oversight of the region assumes the role of the Legat under this subsection.

for the activity as required by host country law), unless the FBIHQ operational division HOC specifies otherwise. Provide input on whether justification exists for granting an exception to host country notification.

- (U//FOUO) For criminal matters, notify any relevant U.S. partner LE agency (e.g., the DEA) operating within the host country, when applicable, regarding the CHS's operation and facilitate the coordination of activity, if appropriate, in coordination with the FBIHQ operational division HOC.
- (U//FOUO) Process and cover Sentinel information leads for CHS personal, business professional, and transit travel. Consult the FBIHQ operational division HOC or the HCC IOD representative of concerns or to request that operational approval be obtained.
- (U//FOUO) Review and cover Sentinel information leads for CHS travel and ET activity, including operational travel, ET resident, ET communications, and third-country debrief. Conduct a Sentinel document review of the CHS ET Activity Package and inform the operational division HOC of any issues with the operational request, such as in-country coordination problems, elevated risk scenarios, or a significant foreseeable reason to delay the activity.
- (U//FOUO) Monitor Sentinel CHS travel and ET activity tasks to receive HOC-approved text suitable for dissemination to in-country USG and/or foreign partners. The HOC will obtain foreign dissemination request (FDR) approval for host nation notification.
- (U//FOUO) Process CHS travel and ET activity Tasks by creating LHMs, conducting requisite in-country notifications, and providing the status of requested notifications.
- (U//FOUO) Coordinate travel requests with the HCC, as needed.

### 19.7. (U//FOUO) Role of the International Operations Division in ET CHS Operations

(S//NF) Once the appropriate IOD geographic unit receives notification from the FBIHQ operational division HOC of the ET operation request, the IOD geographic unit must ensure that the ET operation of the CHS does not conflict with or potentially impair other FBI operations underway in the CHS AOR. The IOD geographic unit must also:

- (S//NF) Coordinate with the affected Legat(s) on the operational request, as appropriate.
- (S//NF) Provide the FBIHQ operational division HOC and the requesting FO with insight into possible geographical issues that may affect the proposed operation, if any.
- (S//NF) Give the requesting entities a fuller understanding of global intelligence collection priorities and guidance on threat-related activity in the AOR that may be relevant to their operation.
- (U//FOUO) Review and cover Sentinel information leads for CHS personal, business/professional, and transit travel. Consult the FBIHQ operational division HOC or the HCC IOD representative regarding concerns or to request operational approval.
- (U//FOUO) Review and cover Sentinel information leads for CHS ET travel and activity, including operational travel, ET resident, ET communications, and third-country debriefs. Conduct a Sentinel document review of the CHS ET Activity Package and inform the operational division HOC of any issues with the operational request, such as in-country

coordination problems, elevated risk scenarios, or a significant foreseeable reason to delay the activity.

- (U//FOUO) Monitor the Sentinel CHS ET activity tasks, for countries without current Legat coverage, to receive HOC-approved text suitable for dissemination to in-country USG and/or foreign partners. The HOC will obtain FDR approval for host nation notification.
- (U//FOUO) Process CHS ET activity tasks, for countries without current Legat coverage, by creating LHMs, conducting requisite in-country notifications, and providing the status of requested notifications.

(S//NF) For requests that include a request for an exemption of notification to the Legat, the IOD geographic unit must assist the FBIHQ operational division HOC with facilitating AD, IOD approval of the request in accordance with subsection 19.15., "Exemption to Providing Legat Notification."

### 19.7.1. (U) International Operations Division Approval and Management Role Over LEGAT- or ALAT-Assigned ET CHS

(U//FOUO) Whenever a LEGAT or an ALAT seeks to open and operate an ET CHS pursuant to this section, IOD management assumes the role, authorities, and responsibilities of FO management, as detailed in this PG. Moreover, all standards, requirements, notifications, and approvals for opening and operating a CHS apply to a Legat or an ALAT, unless specifically exempted in this PG. These polices include, but are not limited to, requirements for opening a CHS, operating a CHS in an ET environment, admonishing a CHS, paying a CHS, documenting CHS contact, and conducting CHS file reviews, among other activities.

(U//FOUO) Accordingly, the following equivalent roles are established for IOD management:

- (U//FOUO) Wherever the CHS policy mandates SSA approval, the UC of the IOD unit responsible for that Legat is the approving official.
- (U//FOUO) Wherever the CHS policy mandates ASAC authority, the IOD SC is the approving official.
- (U//FOUO) Wherever CHS policy mandates SAC authority, the IOD DAD is the approving official.
- (U//FOUO) Wherever CDC authority is required, IOD must seek authority from the OGC.

(U//FOUO) IOD must designate a CHSC, who will assume the same role, authorities, and responsibilities as CHSCs in FOs (see subsection 2.1.2., "Confidential Human Source Coordinator").

## 19.8. (U) ET CHS Operations by a LEGAT or an ALAT

(S//NF) A request for the LEGAT or ALAT to open a CHS in a foreign country must be made in support of an open full substantive national security, PFI, or criminal investigation. A Legat may not be the OO for a full substantive investigation. A full 163 classification is not considered a substantive investigation, and therefore is not permitted as the basis for opening a CHS overseas.

(U//FOUO) The opening request must be made in accordance with the procedures described in Section 4, "Opening and Reopening a Confidential Human Source," and Section 5, "Confidential

Human Source Admonishments," and approved by the appropriate IOD UC. The opening communication must also document that the LEGAT or ALAT has coordinated with the FO squad, task force, or other FBI entity assigned to the full investigation. This information must include the FO personnel contacted, their role in the full investigation, and their support of the CHS opening and subsequent operation to support the FO investigation. Additionally, based upon the nature of the full investigation, the LEGAT or ALAT should provide the FO agent or TFO assigned to the FO investigation with administrative access to the CHS Delta file to ensure that the FO and LEGAT/ALAT are closely coordinating on taskings to the CHS and all actionable intelligence received from the CHS.

(U//FOUO) Concurrently with the above approval to open the CHS, the IOD unit with oversight responsibility for the Legat must submit a request for the LEGAT or ALAT to operate the ET CHS using the [redacted] to the IOD geographic unit UC for approval and must seek approval from the operational division AD with program responsibility for the full investigation that the CHS is supporting. The request to conduct operational activity must be documented in accordance with approval and notifications requirements detailed in subsection 19.4., "Documentation Requirements for All CHS ET Operational and Communication Requests," and other relevant subsections of this PG. The approval is obtained using the [redacted] workflow; in the circumstance of a Legat operating a foreign CHS, the category is most likely "Foreign Resident."

(S//NF) Prior to a LEGAT's or an ALAT's external dissemination of information that was obtained from a CHS assigned to the LEGAT or ALAT and is related to a pending FBI criminal or national security investigation, the information must be reviewed by the appropriate IOD unit and the affected FO squad, task force, or other FBI entity to ensure that the information is deconflicted with other known information and is of value to intended recipients. The IOD geographic unit and affected FO(s) must respond to the LEGAT request to review the proposed dissemination no more than five business days from the time notification is sent by the LEGAT; otherwise, the information is disseminable through an approved FBI dissemination process.

### 19.8.1. (U//FOUO) LEGAT or ALAT Access to a Field Office CHS File

(U//FOUO) Whenever an FBI CHS resides or is located in a foreign country for 60 or more consecutive days, the FO assigned to the CHS should coordinate with the country's LEGAT to determine whether the LEGAT or ALAT should be provided administrative access to the CHS file. This designation is discretionary and is determined by the FO based upon the type of CHS reporting, the host country threat level, and other relevant operational factors related to the CHS.

## 19.9. (U) Employee Travel Related to a CHS Operation

(S//NF) If an employee travels to a foreign country in connection with the operation of a CHS, the employee must send the following information with action leads to the appropriate operational division HOC, IOD geographic unit, and Legat(s) in an SAC-approved EC, with a reference to the separate [redacted][22]

[22] If the travel involves a non-agent employee, the approving official must consider not only security risks related to the in-country environment, but also operational risks associated with interacting with a CHS in a controlled or public setting.

- (U//FOUO) Official Bureau name or AFID[23]
- (U//FOUO) Purpose of travel (e.g., meetings, CHS debriefings)
- (S//NF) Cover status, if applicable
- (U//FOUO) Probable itinerary (i.e., travel schedule, flight numbers, hotels)
- (U//FOUO) Passport type, number, and expiration date
- (U//FOUO) Previous travel to country (including permanent assignments, TDYs, and personal travel)
- (U//FOUO) City or location where the employee may be operationally active
- (U//FOUO) Time period of operational activity
- (U//FOUO) Hotels used operationally
- (U//FOUO) Cellular telephone to be used and anticipated use of any technical equipment
- (U//FOUO) Whether the employee will need access to or assistance from the station, an embassy, or a consulate

(U//FOUO) As soon as known, flight and lodging itinerary must be provided to the operational division HOC and the Legat.

(U//FOUO) The EC must request country clearance from the Legat and provide details on the purpose of the official travel (see Bullet 2 above). Separately, the employee must submit a DOS electronic country clearance (eCC) via the Internet through the DOS's Web page. Specific requirements for obtaining country clearance are provided on the IOD Intranet site.

(S//NF) The employee should only list [redacted] since foreign nationals often process the request form.

(U//FOUO) The employee must also complete the internal [redacted]

(U//FOUO) The above employee travel request and approval communication content must be classified as appropriate for the investigative activity to be undertaken, and it must be serialized into the substantive investigative file the employee is traveling to support.

### 19.9.1. (S//NF) Special Agent Undeclared Travel

(S//NF) The purpose of this subsection is to establish a means to meet with and debrief an open CHS in a foreign country while protecting both the CHS's and and the SA's USG affiliations. In this regard, the below-described activity is not undercover activity, since it is not designed to collect intelligence or obtain evidence from a subject of an investigation or to engage in any operational activity, including CHS taskings. Rather, it is conducted in furtherance of an open CHS file supporting a domestic investigation, and the activities are solely related to debriefing and administrative support of the foreign-based CHS. Agents must be cognizant that activity under this subsection is authorized pursuant to ET CHS authorities and is not governed by other

---

[23] As noted earlier in the section, all provisions of the PG apply unless stated otherwise. Nevertheless, it is important to emphasize that subsection 2.2.3., "Non-Agent Investigative Staff," applies to FBI non-agent operational staff extraterritorially. Moreover, [redacted] must only be used in support of a CHS-related meeting or debriefing activity.

criminal or national security ET operational guidelines for employees. Therefore, no operational activity, including undercover activity, is permitted when traveling pursuant to this subsection.

(S//NF) In support of an FBI or USIC objective, the necessity may arise for an SA to travel overseas in an undeclared manner to debrief, train, or assess an already-open CHS in a foreign country (generally used in a third country where the CHS does not operate) [redacted]

[redacted]

(S//NF) At the initiation of any plan for an SA to travel undeclared for a CHS-related debriefing, the SA must contact the appropriate operational division HOC to receive instructions and guidance on tradecraft used for undeclared travel and for assistance in planning this travel. No travel-related activity is permitted by the SA for the undeclared travel without prior consultation with the appropriate operational division HOC, which will evaluate the proposal and conduct predeployment coordination with IOD counterparts and the relevant Legat(s) to identify and resolve possible issues. All undeclared travel (i.e., official operational travel [redacted] without disclosing FBI affiliation) must be approved via [redacted] with the information listed in subsection 19.10., "ET Admonishments," by the FO SAC, the AD of the operational division (nondelegable) with program oversight of the activity, and the appropriate IOD SC (nondelegable). Prior to travel, the employee must also complete the [redacted]

(S//NF) Due to the nature of undeclared travel, it may not always be feasible for the SA to obtain receipts for expenses incurred during the travel. Therefore, whenever a receipt is not obtained, Federal Travel Regulation (FTR) procedures or the reimbursement certification steps described in Section 17 will suffice as the means to seek reimbursement for purchases made or expenses incurred in support the undeclared travel. All funding associated with undeclared travel must be paid through FO case funds or a travel authorization number provided by FBIHQ. Questions from the FO regarding whether an expense should be reimbursed must be brought to the attention of the SSA assigned to the operational division HOC for review and resolution.

### 19.10. (S//NF) ET Admonishments

(S//NF) Prior to the CHS's ET operation, an FBI SA and an additional FBI SA or other government official, present as a witness, must review with the CHS the admonishments listed below. These admonishments must be reiterated at least annually, but may be provided more frequently, as deemed appropriate by the SA. The admonishments listed below are separate and in addition to the required opening and annual AGG-CHS admonishments described in the Section 5, "Confidential Human Source Admonishments." The ET admonishments are as follows:

- (S//NF) Unless authorized by the FBI, the CHS must not engage in illegal conduct in violation of the laws of the United States or of the host country.

- (S//NF) The CHS is subject to arrest and prosecution for all violations of host nation laws.
- (S//NF) The CHS, if subject to U.S. law, may be arrested and prosecuted for all violations of U.S. laws, unless the violation of these laws is authorized by the FBI.
- (S//NF) The CHS may take responsible measures of self-defense in order to protect his or her own life or the lives of others. These measures, however, may be undertaken only when it is not possible to obtain protection from LE authorities. The CHS must make every reasonable effort to contact and inform the FBI of the self-defense measures taken as soon as possible.
- (S//NF) If it becomes necessary, in an emergency situation, for the CHS to participate in an activity that is illegal or requires AG approval and for which the CHS does not have the proper authorization (e.g., a sensitive circumstance), the CHS must make every reasonable effort to contact the FBI in advance of the activity in accordance with the emergency plan described in the CHS travel or operations request.
- (S//NF) If the CHS is arrested or detained as a result of activities undertaken on behalf or at the request of the FBI, including OIA, circumstances may be such that neither the FBI nor the DOJ can provide any assistance in resolving the situation.

(U//FOUO) If the ET admonishments cannot be performed in person, secure communication protocols must be utilized in accordance with subsection 10.2., "Electronic Communications with a CHS." After the admonishments are provided, the SA and witness must document that the admonishments were given and the CHS acknowledged and understood them. The admonishments must be placed into the CHS's validation sub-file. The admonishments must be placed into the CHS file.

### 19.11. (U) Pre-Operational CHS ET Briefs and Planning

(S//NF) A CHS should also be thoroughly briefed on taskings, the communication plan while in-country and upon return to the United States, the emergency communication plan, the exfiltration plan, and the cover story for the operational travel, as needed. Other travel-related issues and any safety considerations should be covered with the CHS to ensure that the CHS is situationally aware of the threat environment.

### 19.12. (U//FOUO) CHS Payments

(U//FOUO) Payments to a CHS engaged in ET operations must be in accordance with subsection 17.7., "Payment Requests," subsection 17.8., "Payment Approvals," and subsection 17.9., "Paying a CHS."

### 19.13. (U//FOUO) Emergency ET OIA Authorization

(S//NF) If it becomes necessary for a CHS to participate in OIA that was not foreseen or anticipated, he or she must make every reasonable effort to contact the FBI in advance of the activity. The appropriate operational division, in turn, must make every reasonable effort to contact the AG or AG's designee if the OIA in which the CHS needs to participate would require the approval of that entity. If the advance contact with the FBI and/or DOJ is not feasible in the face of an imminent threat to life or physical safety or the imminent compromise of a CHS or an operation where national security would be seriously endangered, the CHS may participate in the OIA so long as he or she does not take part in, and makes every effort to prevent, any act of

violence. An act of violence is any activity that might cause serious bodily injury to another person. These provisions do not prevent a CHS from taking reasonable self-defense measures in an emergency in order to protect his or her own life or the lives of others. Upon learning of this activity, the FBI employee must report the activity to the SAC as soon as possible. The SAC, in turn, must submit the report to the appropriate operational division HOC, IOD geographic unit, and Legat. The operational division HOC must then promptly inform the AG, or AG's designee, if AG approval would have been required.

### 19.14. (U) Duration of ET OIA Authorization and Request for Renewal

(U//FOUO) Approval for any CHS's participation in ET OIA during a criminal investigation or a national security investigation is valid for a period of up to one year. A request for renewal of OIA authorization may be submitted prior to the expiration of the period, and there is no limit on the number of renewals. If the need arises for CHS participation in OIA of a different type, magnitude, or location from what was approved, a new request must be approved at the proper authority level, as set forth in subsection 19.2.1., "ET OIA by a CHS in Support of a National Security Investigation," and subsection 19.3.4., "ET OIA by a CHS in Support of a Criminal Investigation."

#### 19.14.1. (U) Suspension and Revocation of ET OIA Authorization

(U//FOUO) See subsection 13.7., "Suspension of OIA Authorization," and subsection 13.8., "Revocation of OIA Authorization."

### 19.15. (U) Exemption to Providing Legat Notification

(S//NF) The Legat is the FBI's representative in the host country, establishing and maintaining relationships with both the host country authorities and U.S. LE and intelligence communities in that country. It is essential, therefore, that the Legat be notified and made fully aware of all CHS ET operations and travel in the host country operation.

(S//NF) An exemption to providing this notification requires compelling justification and internal FBI approval, as described below. The FO must request an exemption to Legat notification via an EC, using the respective operational division HOC's restricted Legat exemption case file in Sentinel. Upon receipt of the request, the HOC must coordinate the request among the field and FBIHQ entities. It is strongly recommended that the requesting SA seek guidance from the appropriate FBIHQ unit representative prior to preparing the [redacted] must not be used to request ET operational activity authorization when seeking this exemption. The EC must include specific facts showing that the circumstances of the travel or operation are so extraordinarily sensitive that the Legat's knowledge of the investigation or operation would likely jeopardize the operation. Additionally, the EC must provide all relevant details about the CHS operation that would normaly be addressed in the [redacted]

(S//NF) If approved, the CHS travel must be coordinated directly with CIA Headquarters through the operational division HOC, and the COM must be notified of the activity if the COM notification is appropriate for the operational circumstances.

(S//NF) The required approvals, to be issued via EC, for granting an exemption to the Legat notification requirement are as follows:

- (S//NF) SAC approval

- (S//NF) Operational division AD approval
- (S//NF) IOD AD approval

### 19.16. (U) Special Circumstances

(S//NF) A special circumstance is a rare occasion in which a CA or co-CA must open, operate, and pay an individual for services, expenses, or both for a limited time, prior to adhering to the requirements set forth in this PG, such as those set for opening a CHS in Delta, for approval of ET operations, and for admonishing the CHS. Such circumstances could arise, for example, in a war zone or other hostile environment.

(S//NF) In these circumstances, the CA or co-CA still must make a reasonable effort to ascertain the trustworthiness of the individual, obtain verbal approval to operate and pay the individual, and provide appropriate admonishments to the individual.

(S//NF) Within 30 days of tasking the individual, the CA or co-CA is responsible for ensuring that the individual is opened as a CHS in Delta and that all requisite written approvals, notifications, and admonishments have been obtained and documented, including a history of the taskings issued, the information received, and the validation conducted, as set forth in this PG and the [redacted]

### 19.17. (U//FOUO) Use of an ET Sub-Source

(U//FOUO) In ET operations, the FBI's use of an ET sub-source is permitted. See subsection 10.12., "Use of a Sub-Source" for the definition of a sub-source.

### 19.18. (U) Communications About a CHS

(U//FOUO) Communications between FBI personnel and others in the LE or intelligence community regarding CHSs must be conducted using a secure method (e.g., secure fax, secure telephone, secure e-mail). Note that the FBI unclassified network (UNet) is not secure.

(S//NF) If any personally identifiable information (PII) belonging to the CHS is released, including any selectors, a [redacted] form must be completed and maintained in the CHS file, and the CA or co-CA must obtain the CHS's concurrence prior to releasing the CHS's identity to a non-FBI agency or foreign government.

(S//NF) An FDR may also need to be sought from the operational division HOC (or its functional equivalent).

### 19.19. (U) ET Unauthorized Illegal Activity

(S//NF) Whenever any employee learns of CHS participation in any act of violence, the employee must immediately notify the CHSC, the employee's supervisor, and the SAC. The SAC, in turn, must notify the operational division AD and the [redacted] SC of the facts and circumstances, using the list provided below as a guide. Any determination to continue to use the CHS must be approved by the Director (or designee), in consultation with DOJ's Criminal Division or NSD, as appropriate.

(S//NF) As soon as possible, the SA must notify in writing the operational division, appropriate IOD geographic unit, and Legat of any ET UIA by a CHS. The written notification must be retained in the CHS validation sub-file and must address the following factors:

- (S//NF) Whether the activity is ongoing or complete

- (S//NF) Whether specific charges were brought against the CHS, including the type(s) of violation, if any
- (S//NF) Details surrounding the CHS's participation in the UIA, including the degree and nature of the CHS's participation and the seriousness of the activity in terms of damage to life and to property
- (S//NF) Whether the UIA was related to the CHS's tasking by the FBI; and if so, in what manner
- (S//NF) Whether the CHS's relationship with the FBI has been revealed or confirmed to any outside agency as a result of the CHS's participation in UIA and, if so, details of the disclosure
- (S//NF) Whether any attempt has been made or will be made to intercede on behalf of the CHS, or whether any request or recommendation has been made to any foreign LE authorities
- (S//NF) The SAC's decision regarding whether to continue operating the CHS, a justification supporting the decision and, if applicable, the opinion of the AUSA

(U//FOUO) For the purposes of ET criminal CHS operations, UIA refers to activity illegal under U.S. federal, state, or local law and the laws of a host country. UIA during ET national security CHS operations does not include violations of host country law. UIA also does not include CHS activity tasked by the FBI for which the FBI was required to obtain, but failed to obtain, proper OIA authorization.

(S//NF) Since the UIA is relevant to validation factors, the activity must be documented in the FOASR. The CA may have the option of submitting the FOASR in support of an out-of-cycle validation request if there are concerns regarding the CHS's continued use (see [redacted]

(U//FOUO) If a CHS self-reports UIA, the CA must immediately notify the Legat, IOD geographic unit, and the operational division HOC via an EC. If the activity described would have required AG approval, the operational division must notify DOJ.

### 19.19.1. (U) Unauthorized Illegal Activity Notification to DOJ

(S//NF) For criminal operations, the operational division must promptly notify the AG (or designee), through contact with the AAG for the Criminal Division, of any serious violation of law, or violations of law which, in criminal operations, would constitute sensitive circumstances as defined in subsection 19.3.3., "ET CHS Operations in Support of Criminal Investigations Involving Sensitive Circumstances," by a criminal CHS. This includes serious charges or an arrest on such activity by any international or foreign LE agency. After consultation with all affected USG entities, the [redacted]SC will decide what action, if any, should be taken with respect to the violation(s), short of prosecution. This includes the decision of whether or not to continue the source relationship with the CHS. Any decision as to a potential prosecution will be made by DOJ on a case-by-case basis.

(S//NF) For national security matters, whenever an FBI employee receives credible information concerning UIA by a national security CHS, whether or not the activity occurred in connection with the FBI-authorized operation or tasking, the employee must notify his or her supervisor and

the SAC. The SAC, in consultation with the operational division AD (or designee), may determine to authorize continued participation in that activity by the CHS in accordance with the national security OIA procedures detailed in this section. The requirement to report the UIA to the AG (or designee) through contact with the AAG for NSD applies only if the SAC, after consultation with the [redacted] SC, decides not to approve the CHS's participation in the activity. If the determination is made not to approve the activity, the UIA must be communicated to DOJ using a document suitable for dissemination.

**19.20. (S//NF) International Incidents**

(S//NF) An international incident is defined as any incident that may potentially damage U.S. foreign relations. International incidents include circumstances that could have a significant adverse impact on foreign relations or LE activities and affect U.S. interests anywhere, including matters such as treaty negotiations, extraditions, drug interdiction efforts, and litigation in foreign, domestic, or international courts. An international incident does not generally include the arrest of a CHS. However, a reported arrest must be reviewed to determine the extent of UIA involved. See subsection 19.19., "ET Unauthorized Illegal Activity."

(S//NF) If a CHS notifies an FBI employee that the CHS was involved in an international incident, the FBI employee to whom the notice is given must immediately notify the appropriate Legat, IOD geographic unit, operational division HOC, and, if applicable, the AUSA involved in the operation of the CHS. The operational division HOC is responsible for notifying the AG or AG's designee of the incident as soon as possible, as well as the CIA and the DOS, if appropriate.

## 20. (U) Confidential Human Source Validation

(U) Until updated guidance on CHS validation standards policy is issued, please refer to the [redacted]

# Appendix A: (U) Final Approvals

| POLICY TITLE: (U) *Confidential Human Source Policy Guide* | |
|---|---|
| **Primary Strategic Objective** | P4–Collection |
| **Publish Date** | 2015-09-21 |
| **Effective Date** | 2015-09-21 |
| **Review Date** | 2018-09-21 |
| **EXEMPTIONS** | |
| None | |
| **REFERENCES** | |
| See Appendix B. | |
| **APPROVALS** | |
| **Sponsoring Executive Approval** | **Rafael J. Garcia, Jr.**<br>Assistant Director<br>Directorate of Intelligence |
| **Final Approval** | **Eric Velez Villar**<br>Executive Assistant Director<br>Directorate of Intelligence |

# Appendix B: (U) Sources of Additional Information

- (U) [redacted]
- (U) [redacted]
- (U) NHMD 006.08, *Intelligence Community Directive 304 – Human Intelligence Clandestine Operational Coordination Procedures*
- (U) NHMD 006.08, Annex C, "Principles for Joint Source Handling"
- (U) Counterterrorism HUMINT Operations Unit (CHOU) Intranet site

# Appendix C: (U) Contact Information

| Division | Directorate of Intelligence |
|---|---|
| Section | Strategic Services Section |
| Unit | Standards and Practices Unit<br>J. Edgar Hoover Building<br>935 Pennsylvania Avenue, NW<br>Washington, DC 20535 |
| Point of Contact | Unit Chief<br>[redacted] |

# Appendix D: (U) Acronyms

| | |
|---|---|
| AAG | assistant attorney general |
| AAR | after-action report |
| ACS | Automated Case Support |
| AD | assistant director |
| ADIC | assistant director in charge |
| AFID | alias/false identification |
| AFOSI | Air Force Office of Special Investigations |
| AG | Attorney General |
| AGG | Attorney General's guidelines |
| AGG-CHS | *The Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources* |
| AGG-Dom | *The Attorney General's Guidelines for Domestic FBI Operations* |
| AGG-UCO | *The Attorney General's Guidelines for Federal Bureau of Investigation Undercover Operations* |
| AHOC | Advanced HUMINT Operation Course |
| ALAT | assistant legal attaché |
| AMU | Asset Management Unit |
| AOR | area of responsibility |
| ASAC | assistant special agent in charge |
| AUSA | assistant United States attorney |
| BAT | Behavioral Assessment Team |
| BCC | border crossing card |
| BOP | Bureau of Prisons |
| CA | case agent |
| CBP | Customs and Border Patrol |
| CD | Counterintelligence Division |
| CDC | chief division counsel |
| CE | case expenditures |

| | |
|---|---|
| CFP | chief federal prosecutor |
| CFPG | *Confidential Funding Policy Guide* |
| CFR | confidential file room |
| CHOU | Counterterrorism HUMINT Operations Unit |
| CHS | confidential human source |
| CHSC | confidential human source coordinator |
| CI | counterintelligence |
| CIA | Central Intelligence Agency |
| CollMC | collection management coordinator |
| COM | chief of mission |
| COS | chief of station |
| CPI | crime problem indicator |
| CPS | CHS Prioritization System |
| CRIM | criminal |
| CTD | Counterterrorism Division |
| CTS | Counterterrorism Section |
| CYB | cyber |
| CyD | Cyber Division |
| DA | double agent |
| DAD | deputy assistant director |
| DAG | deputy attorney general |
| DCID | Director of Central Intelligence Directive |
| DD | Deputy Director |
| DEA | Drug Enforcement Administration |
| DHCC | Domestic HUMINT Collection Course |
| DHS | Department of Homeland Security |
| DI | Directorate of Intelligence |
| DIOG | *Domestic Investigations and Operations Guide* |
| DIVS | Data Integration and Visualization System |

| | |
|---|---|
| DNI | Director of National Intelligence |
| DoD | Department of Defense |
| DOE | Department of Energy |
| DOJ | Department of Justice |
| DOS | Department of State |
| DT | domestic terrorism |
| EAD | executive assistant director |
| EC | electronic communication |
| ECC | electronic country clearance |
| ECPA | The Electronic Communications Privacy Act |
| ELSUR | electronic surveillance |
| EO | executive order |
| ERISA | Employee Retirement and Income Security Act |
| ERO | Enforcement and Removal Operations |
| FAMS | FBI Automated Messaging System |
| FBI | Federal Bureau of Investigation |
| FD | Finance Division |
| FDR | foreign dissemination request |
| FIG | Field Intelligence Group |
| FinCEN | Financial Crimes Enforcement Network |
| FISA | Foreign Intelligence Surveillance Act |
| FO | field office |
| FOASR | Field Office Annual Source Report |
| FOUO | For Official Use Only |
| FPO | Federal Prosecuting Office |
| FSO | foreign service officer |
| [redacted] | [redacted] |
| FTC | Field Tradecraft Course |
| FTR | Federal Travel Regulation |

| | |
|---|---|
| HCC | HUMINT Coordination Center |
| HEAT | HUMINT Evaluation and Assessment Team |
| [redacted] | [redacted] |
| HOC | HUMINT Operations Center |
| [redacted] | [redacted] |
| [redacted] | [redacted] |
| HQ | headquarters |
| HSI | Homeland Security Investigations |
| HSRC | Human Source Review Committee |
| [redacted] | [redacted] |
| HSVR | Human Source Validation Report |
| HUMINT | human intelligence |
| IA | intelligence analyst |
| IAO | International Affairs Office |
| IC | Intelligence Community |
| ICE | Immigration and Customs Enforcement |
| IIR | intelligence information report |
| IMF | International Monetary Fund |
| INR | Bureau of Intelligence and Research |
| IO | intelligence officer |
| IOB | Intelligence Oversight Board |
| IOD | International Operations Division |
| IRSU | Intelligence Research Support Unit |
| IT | international terrorism |
| JTTF | Joint Terrorism Task Force |
| LE | law enforcement |
| LEGAT | legal attaché (position) |
| Legat | legal attaché (office) |
| LEO | law enforcement officer |

| | |
|---|---|
| LEPU | Law Enforcement Parole Unit |
| LHM | letterhead memorandum |
| LPR | legal permanent resident |
| M&IE | meals and incidental expenses |
| MAIA | Managed Attribution Internet Access |
| MD | Doctor of Medicine |
| MDCO | Military Department Counterintelligence Organization |
| MET | Mobile Evaluation Team |
| MOU | memorandum of understanding |
| MTR | Mandatory Tracking Review |
| NARA | National Archives and Records Administration |
| [redacted] | [redacted] |
| NCIC | National Crime Information Center |
| NCIS | Naval Criminal Investigative Service |
| NFPO | No Foreign Policy Objection |
| NHMD | National HUMINT Manager Directive |
| NOFORN | Not Releasable to Foreign Nationals |
| NOR | notice of request |
| NSD | National Security Division |
| NSICG | *National Security Information Classification Guide* |
| NSL | National Security Letter |
| OCA | Office of Congressional Affairs |
| OEO | Office of Enforcement Operations |
| OGA | other government agency |
| OGC | Office of the General Counsel |
| OIA | otherwise illegal activity |
| OO | office of origin |
| OPR | Office of Professional Responsibility |
| OTD | Operational Technology Division |

| | |
|---|---|
| PD | policy directive |
| PED | portable electronic device |
| PFI | positive foreign intelligence |
| PG | policy guide |
| PGI | project-generated income |
| PII | personally identifiable information |
| PINS | Public Integrity Section |
| PM | program manager |
| POC | point of contact |
| POL | pattern of life |
| PR | pen register |
| QAN | query alert notification |
| QSSR | Quarterly Supervisory Source Report |
| RFF | request for files |
| RFI | request for information |
| RIP | recruitment-in-place |
| ROU | Remote Operations Unit |
| SA | special agent |
| SAC | special agent in charge |
| SC | section chief |
| SecD | Security Division |
| SES | Senior Executive Service |
| SIA | supervisory intelligence analyst |
| SIM | sensitive investigative matter |
| SIP | Source Identification Package |
| SPBP | Significant Public Benefit Parole |
| SSA | supervisory special agent |
| SSI | source sensitive information |
| SSIA | senior supervisory intelligence analyst |

| | |
|---|---|
| SSN | social security number |
| TDY | temporary duty |
| TECS | Treasury Enforcement Communications System |
| TFO | task force officer |
| TSA | Transportation Security Administration |
| TT | trap and trace |
| U.S. | United States |
| U.S.C. | United States Code |
| UC | unit chief |
| UCC | undercover coordinator |
| UCE | undercover employee |
| UCO | undercover operation |
| UESU | Undercover Employee Safeguard Unit |
| UFMS | Unified Financial Management System |
| UIA | unauthorized illegal activity |
| UN | United Nations |
| UNet | Unclassified Network |
| UNI | Universal Index |
| USAO | United States Attorney's Office |
| USCIS | United States Citizenship and Immigration Services |
| USG | United States government |
| USIC | United States Intelligence Community |
| USMS | United States Marshals Service |
| USPER | United States person |
| USSG | United States Sentencing Guidelines |
| [redacted] | [redacted] |
| VOIP | Voice Over Internet Protocol |
| VOTU | Validation Operational Testing Unit |
| VS | Validation Section |

| | |
|---|---|
| WFO | Washington Field Office |
| WHO | World Health Organization |
| WMD | weapon of mass destruction |
| WMDD | Weapons of Mass Destruction Directorate |
| WSP | Witness Security Program |

# Appendix E: (U) TS//SCI CHS Reporting

**(U) Overview of [redacted]**

(U//FOUO) [redacted] is the FBI record management system established to maintain information reported by a CHS that must be categorized as Top Secret (TS) or Sensitive Compartmented Information (SCI) [redacted] used in conjunction with Delta, provides all FBI employees who receive TS and SCI information from a CHS with the capability to document, handle, store and access the information.

**(U) Requirements and Procedures for the Use of [redacted]**

(U//FOUO) [redacted] must be utilized to document and store TS and SCI information obtained from a CHS. The procedures for requesting access to [redacted] and maintaining CHS reporting in the [redacted] system are provided on the [redacted] Intranet page.

**(U) Requirements for Closing a CHS File/Folder in [redacted]**

(U//FOUO) When a source is closed, his or her [redacted] folder will be marked as closed, and details about the closure of the source will be entered into [redacted] The [redacted] source folder will be marked with an electronic flag in [redacted] and moved to another location within [redacted] will use a SharePoint-based computing service to store closed sources. Any source folder for a closed source must be moved to the [redacted] SharePoint RCS within one year of deactivation. The CA is responsible for ensuring that deactivated source folders are moved to the SharePoint RCS. HPMU will conduct a biannual review.

# Appendix F: (U) Service Agreement

**Mandatory Language:**

SERVICE AGREEMENT

Whereas the Federal Bureau of Investigation, hereinafter referred to as the FBI, is conducting a lawful investigation regarding activities on the part of individuals engaged in the violation of various United States (insert type—e.g., criminal) statutes.

Whereas (CHS's payment name) is in a position to and is willing to furnish assistance to the FBI in its investigation; and

Whereas the parties hereto desire to record their respective interests and obligations,

Now, therefore, the parties hereto agree as follows:

RESPONSIBILITIES OF PARTIES

In furtherance of the goals of the aforementioned investigation, (CHS's payment name) will provide information on the (insert program type—e.g., criminal) activities of various (insert type of case—e.g., white supremacy and/or domestic terrorism subjects).

(CHS's initials) will not participate in any unlawful activities, except insofar as the FBI determines that such participation is necessary to this investigation and the FBI expressly authorized these acts. It is understood that any such violations of the law not expressly authorized by the FBI may result in the prosecution of (CHS's payment name). The FBI does not have authority to make any promise or commitment that would prevent the government from prosecuting for illegal acts which have not been specifically and expressly authorized by the FBI.

(CHS's initials) will not initiate any plans to commit criminal acts, nor will he or she participate in any acts of violence. If he or she is asked to participate in any act of violence or learns of such plans, he or she will attempt to discourage those plans or acts and will promptly notify the FBI.

(CHS's initials) is not an employee, partner, member of a joint venture, associate, or special agent of the FBI, nor will he or she identify him- or herself or hold him- or herself out to be such. Notwithstanding this provision, (CHS's initials) may be considered an employee of the United States government, as defined in 28 United States Code (U.S.C.) Section (§) 2671, for the limited purpose of defending civil claims arising out of allegations of wrongful or negligent acts or omissions related to any activity conducted by (CHS's payment name) in furtherance of the aforementioned investigation.

(CHS's payment name) shall have no authority, actual or implied, to obligate and/or bind the FBI to any contractual duty and/or obligation, and any obligations so made are the sole obligations of (CHS's payment name) and not of the FBI.

It is understood that the FBI at its sole discretion will control all investigative activities, including any decision to terminate this investigation.

LIABILITY OF PARTIES

It is expressly understood that the FBI assumes no responsibility or liability to (CHS's payment name) for any income loss, harm to professional reputation or personal reputation, or any other personal damages, property damage, or losses which may arise as direct or indirect consequence

of (CHS's payment name) providing voluntary cooperation in furtherance of the aforementioned investigation. (CHS's payment name) agrees to hold harmless the FBI, its agents, employees, and contractors for any and all liability for damages resulting directly or indirectly there from, except as set forth in this agreement. This provision shall survive the expiration or termination of this agreement or of the investigation.

The liability for any negligent acts of the FBI and its agents, employees, and contractors will be borne by the FBI. The liability for any negligent or willful acts or omissions of (CHS's payment name) is the sole responsibility of (CHS's payment name). However, (CHS's initials) does not waive the right or claim to which (CHS's payment name) may be entitled under the Federal Tort Claims Act. This provision shall survive the expiration or termination of this agreement or of the investigation.

CONFIDENTIALITY

(CHS's payment name) will in no way reveal the confidential and sensitive nature of this investigation or identify any FBI agents to any unauthorized person or persons; and further, will not undertake any publication or dissemination of any information or material that results from this investigation without the prior express written authorization of the FBI. This provision shall survive the expiration or termination of this agreement or of the investigation.

DURATION OF AGREEMENT

This agreement shall commence on the date of acceptance by (CHS's payment name), as signified by subscription of his or her signature hereto, and shall continue as long as the FBI deems that the services of (CHS's payment name) are required; however, the agreement shall not exceed twelve months from the date of acceptance. (A time period such as 90 days or 6 months from the date of (CHS's payment name) signature may be added, if a shorter termination date is desired.) This agreement is subject to a six-month review and determination for continued services. This agreement may be terminated at any time, by either party, and for any reason by delivery of a written notice to terminate. If either party is unable to provide written notice of termination, oral notice of termination may be given to the other party, provided that after orally terminating the agreement, the terminating party creates a written document detailing (i) the date, time, and recipient of the oral termination, (ii) the method by which termination was conveyed, and (iii) a summary of what was said to terminate the agreement.

This document constitutes the full and complete agreement between (CHS's payment name) and the FBI. Any and all prior agreements, whether written or oral, express or implied, are hereby rendered null and void. Modifications to this agreement will have no force or effect unless and until such modification is reduced to writing and signed by all parties thereto.

The representative for the FBI contracting officer in this agreement is Special Agent (insert CA's name), (insert division).

**"If Applicable" Language:**

[If CHS is supporting a UCO, add language detailing the role the CHS will have in the UCO.]

The FBI will reimburse (CHS's payment name) for expenses incurred by him or her which are deemed by the FBI to be reasonable and in furtherance of this investigation. (CHS's payment name) agrees that, prior to incurring such expenses, he or she will consult with the FBI's designated representative as to the nature and justification for incurring such expenses. (CHS's

initials) agrees to provide vendor receipts for these reimbursements, except where the FBI has determined that obtaining a receipt would endanger (CHS's payment name) or disclose (CHS's initials)'s relationship with the FBI. The FBI has the right to direct (CHS's payment name) not to incur expenses which the FBI deems not to be in furtherance of its investigative goals. If there should be a dispute as to whether an expense was reasonable, the FBI contracting officer of record will be the final arbiter of that dispute.

**Set monthly payment amount:**

The FBI agrees to pay (CHS's payment name) (insert dollar amount) per month for his or her services related to this investigation. The FBI has determined that (insert dollar amount) per month is commensurate with the value of the information or assistance (CHS's payment name) shall provide to the FBI. If at any time the FBI determines in their sole discretion that the value of information or assistance provided by (CHS's payment name) to the FBI is not commensurate with (insert dollar amount) per month, the FBI shall terminate or modify this agreement. Receipt of these funds is contingent upon compliance with the obligation of confidentiality and all aspects of this agreement. (CHS's payment name) acknowledges that these payments are taxable income and that he or she is responsible for payment of all applicable local, state, and federal taxes and/or withholdings.

**Payment monthly amount up to designated limit:**

The FBI agrees to pay (CHS's payment name) up to (insert dollar amount) per month for his or her services related to this investigation. The amount of these monthly payments will be determined at the sole discretion of the FBI and must be commensurate with the value of the information or assistance (CHS's payment name) provides to the FBI. Receipt of these funds is contingent upon compliance with the obligation of confidentiality and all aspects of this agreement. (CHS's payment name) acknowledges that these payments are taxable income and that he or she is responsible for payment of all applicable local, state, and federal taxes and/or withholdings.

(CHS's payment name) agrees, at the direction and under the supervision of the FBI, to meet with designated individuals, and agrees to make or have made by the FBI consensual, visual, oral, and wire recordings of such meetings and related telephone calls, if determined to be safe to do so by both parties. Further, (CHS's payment name) will provide written authorization to the FBI to monitor and record such meetings and conversations prior to such monitoring or recording.

(CHS's payment name) agrees, when directed by the FBI, to testify and furnish all information in his or her possession, custody, or control, which he or she has received during the course of or related to this investigation. (CHS's payment name) understands that if he or she testifies in any court proceeding, his or her identity may be fully revealed and his or her cooperation with the FBI disclosed to the public and the subjects of the investigation.

The FBI does not have the authority to reduce (CHS's payment name) sentence, and the FBI makes no guarantees or promises to (CHS's initials) regarding a sentence reduction. However, at the sole discretion of the FBI, the FBI may advise the proper authorities regarding the extent of (CHS's payment name) assistance and cooperation.

By signing below, the parties herewith acknowledge that they have read, understand, and will abide by the foregoing statements.

| | |
|---|---|
| CHS's Payment Name | Date |

**Witness 1:**

| | |
|---|---|
| Name | |
| Title | |
| Date | |

**Witness 2:**

| | |
|---|---|
| Name | |
| Title | |
| Date | |

| | |
|---|---|
| Contracting Officer for the Federal Bureau of Investigation | Date |